Microsoft

MCITP EXAM
70-685

Windows® 7 Enterprise Desktop Support Technician

Tony Northrup
J.C. Mackin

SELF-PACED

Training Kit

Sample Chapters

To learn more about this book visit Microsoft Learning at:
http://www.microsoft.com/learning/en/us/Book.aspx?ID=13917

Contents

CHAPTER 5

Protecting Client Systems

Any computer that is connected to the Internet faces a barrage of network-based threats in the form of malicious software attacks. These threats are growing in number and sophistication every year, and as an enterprise support technician, you are responsible for protecting client systems from these evolving dangers.

As part of your company's broad defense strategy, you need to know how to configure in Windows 7 the features whose purpose is to protect your clients. Specifically, you need to know how to minimize the risk of damage from malware by implementing User Account Control (UAC) at an appropriate level, by using Windows Defender, and by removing unwanted software if it is discovered.

Exam objective in this chapter:

- Identify and resolve issues due to malicious software.

Lesson in this chapter:

Before You Begin

To perform the exercises in this chapter, you need:

- A domain controller running Windows Server 2008 R2
- A client computer running Windows 7 that is a member of the same domain

REAL WORLD

J.C. Mackin

I often hear people repeating a number of misconceptions about viruses and other malware, and I'm convinced that these misconceptions have lulled users and administrators into a false sense of security about the dangers their systems face. Often these misconceptions are based on an accurate understanding of what *was* the state of malware threats about 10 years ago. But the nature of these threats has evolved significantly, and it continues to evolve. So in the interest of learning how best to defend ourselves today, let's deal with the most common of these misconceptions.

- **"As long as you keep Windows updated, you're fine."**

  It's certainly true that you need to keep Microsoft Windows updated, but you need to keep *all* your software updated. Security holes can be found in applications as easily as they can be found in operating systems, and the security holes in many of these can be exploited to completely compromise a system. Microsoft Office applications in particular are often targeted. Remember that your systems are not safe from exploits if you are keeping only Windows updated.

- **"As long as you aren't tricked into opening anything, you're fine."**

  A long time ago, it was true that malicious software needed user assistance to be installed on a system. Now, the situation is completely different. Merely browsing to the wrong site, for example, can lead to a secret drive-by download of malicious software. Even worse, some of the most harmful attacks come from Internet worms, which need no user involvement whatsoever. It is still essential for users to avoid opening unknown software, but this preventative measure alone is not enough to keep your systems safe from infection.

- **"As long as you keep your antivirus software up to date and scan daily, you're fine."**

  This might be the most common of all misconceptions regarding malware. While it's true that a robust anti-malware solution is one of the essential pillars of a sound client protection strategy, the sad truth is that such software has its limitations. Malware developers who are serious about exploiting computers naturally design their programs in a way that avoids detection by antivirus solutions. For example, a rootkit is a relatively new type of malware that—so far—few anti-malware applications have had good success in detecting. But even more familiar types of malware can be designed to evade detection. As a result, when your antivirus software fails to detect malware on a system, you should know that the system still could very easily be infected.

These three misconceptions all have a common thread running through them: the belief that you can protect your systems by adopting a small number of well-known defenses against malware. In truth, adequately protecting client systems requires your company to adopt a wide array of strategies that include effective software updates, antivirus software, user education, firewalls, and most important of all, effective management of these and other security features.

Lesson 1: Resolving Malware Issues

The number of new malware applications being released today actually exceeds that of new legitimate applications. As an enterprise support technician, you need to adequately protect your clients from these mounting threats and know how to handle malware infections once they are discovered.

Windows 7 includes two features that assist you in this fight against malware. User Account Control (UAC) helps prevent programs from secretly altering protected areas of the operating system, and Windows Defender scans your system for spyware and offers to remove any unwanted software that is detected.

Though you will need to use additional applications such as Microsoft Forefront and a managed anti-malware solution to protect your network, understanding how to use and configure these built-in features of Windows 7 represents part of the essential skill set you need on your job.

After this lesson, you will be able to:

- Configure User Account Control (UAC) to display notifications in a way that suits the needs of your organization.
- Configure Windows Defender settings.
- Detect and remove some malware manually in case your anti-malware applications fail.

Estimated lesson time: 30 minutes

Understanding Malware

Malware is an umbrella term for many different types of unwanted software. It's important to understand the nature of these different threats, but it's also important to recognize that many malware applications blend features from more than one of these malware types. The following list discusses the most common types of malware:

- **Virus** A *virus* is a self-replicating program that can install itself on a target computer. Viruses do not propagate over networks automatically; they need to be spread through e-mail or another means. Once installed, viruses usually alter, damage, or compromise a system in some way.
- **Worm** A *worm* is a self-replicating program that can spread automatically over a network without any help from a user or a program such as an e-mail client or Web browser. Worms vary greatly in the potential damage they can cause. Some worms simply replicate and do little other than consume network bandwidth. Others can be used to compromise a system completely.

- **Trojan horse** A Trojan horse is a program that is presented to users as a desirable application but that is intentionally written to harm a system. Unlike viruses and worms, Trojan horses do not copy themselves automatically or install themselves automatically; they rely on users to install them.
- **Spyware** *Spyware* is a type of privacy-invasive software that secretly records information about user behavior, often for the purposes of market research. Typically spyware is injected into a system when a user installs a free tool or visits a Web site with browser security settings set to a low level. The most common function of such spyware is to record the Web sites that a user visits. More rarely, some spyware, such as keyloggers (which record every keystroke), can be installed deliberately by a third party and be used to gather personal information. The biggest threat posed by most spyware is system performance degradation. All types of spyware reduce system performance by hijacking the resources of the computer for their own purposes. Unlike viruses and worms, spyware does not self-replicate.
- **Adware** Adware is similar to spyware and is often installed alongside it. The purpose of adware is to display unsolicited advertisements to the user in the form of pop-up windows or Web browser alterations. Adware can also download and install spyware.

NOTE **SPYWARE AND ADWARE**

The term *spyware* is often used as a general term for all unwanted software that runs in the background and that gathers market research information, displays advertisements, or alters the behavior of applications such as Web browsers. Microsoft uses the phrase "spyware and potentially unwanted software" to refer to the type of software that is unwanted but is not unambiguously harmful.

- **Backdoor** A backdoor is a program that gives a remote, unauthorized party complete control over a system by bypassing the normal authentication mechanism of that system. Backdoors have been known to be installed by worms that exploit a weakness in a well-known program. To protect your system against backdoors, it is essential to keep your applications (not just your operating system) updated.
- **Rootkit** A rootkit is a persistent type of malware that injects itself beneath the application level and that as a result, tends to be much harder to detect from within the operating system. A rootkit can alter the core functionality of the operating system, or it can install itself as its own operating system invisible to the user and to most anti-malware software. Other rootkits can operate at the firmware (BIOS) level. Typically, a rootkit is used to provide a backdoor to a system.

Although malware has been proliferating in type and number, the defenses against these threats have improved as well. When UAC is enabled in Windows 7, for example, a malware application cannot install itself easily without the user's knowledge. This next section provides an overview of UAC, which was introduced in Windows Vista and has been refined in Windows 7.

Understanding UAC

UAC is a set of security features designed to minimize the danger of running Windows as an administrator and to maximize the convenience of running Windows as a standard user. In versions of Windows before Windows Vista, the risks of logging on as an administrator were significant, yet the practice of doing so was widespread. Meanwhile, running as a standard user was generally safe, but the inconveniences prevented many from adopting the practice.

In versions of Windows before Windows Vista, malware could use the credentials of a locally logged-on administrator to damage a system. For example, if you were logged on to Windows XP as an administrator and unknowingly downloaded a Trojan horse from a network source, this malware could use your administrative privileges to reformat your hard disk drive, delete all your files, or create a hidden administrator account on the local system.

The main reason that users in previous versions of Windows often ran as administrators despite these dangers is that many common tasks, such as installing an application or adding a printer, required a user to have administrator privileges on the local machine. Because in previous versions of Windows there was no easy way to log on as a standard user and "elevate" to an administrator only when necessary, organizations whose users occasionally needed administrator privileges simply tended to configure their users as administrators on their local machines.

NOTE **WHAT IS ELEVATION?**

The term *elevation* is used when a user adopts administrator privileges to perform a task.

How Does UAC Address the Problem of Administrator Privileges?

UAC is the result of a new Windows security design in which both standard users and administrators use the limited privileges of a standard user to perform most actions. When users are logged on, UAC prompts them in different ways to confirm actions that make important changes to the computer. If an administrator is logged on, the action is performed only if he or she confirms it. If a standard user is logged on, the action is performed only if he or she can provide administrator credentials. In both cases, the elevation to administrator-level privileges is temporary and used to perform only the action required. Through this new system, UAC inhibits malware from secretly using a logged-on administrator's privileges.

Understanding UAC Notifications for Administrators

By default, UAC is configured to notify administrators only when programs request elevation. For example, administrators see UAC notification when they attempt to run a program (such as Cmd.exe) at elevated administrator privileges, as shown in Figure 5-1. According to this default setting, administrators in Windows 7 do not see a UAC notification when they adjust Windows settings that require administrator privileges.

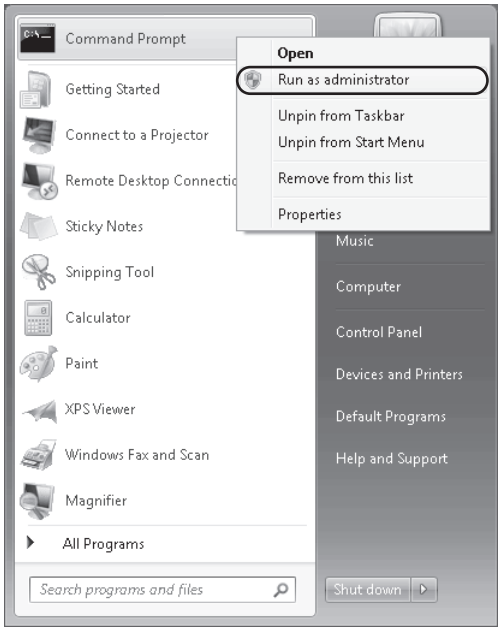

FIGURE 5-1 Opening an elevated command prompt

NOTE **CHANGES IN WINDOWS 7 UAC BEHAVIOR**

For administrators, the default behavior of UAC in Windows 7 has changed significantly from that in Windows Vista and Windows Server 2008. In those operating systems, UAC generated a prompt by default whenever any type of elevation was requested, including when an administrator attempted to change Windows settings. Administrators see UAC prompts less frequently in Windows 7.

The UAC notification that normally appears for administrators is called a *consent prompt* and is shown in Figure 5-2. Note that by default, the entire screen darkens when the notification appears and freezes until the user responds to the prompt. This feature is called the *Secure Desktop* and can be disabled.

NOTE **EDUCATE USERS ABOUT UAC PROMPTS!**

The point of UAC notifications is to alert users when malware might be harming your computer. If malware were to request elevation for a particular purpose, it too would generate a notification such as the one shown in Figures 5-2 or 5-3. Consequently, an essential factor in the ability of UAC to thwart malware is appropriate user response. You need to educate users—and gently remind your fellow administrators—that they should click No or Cancel whenever they see a UAC notification message that they did not initiate.

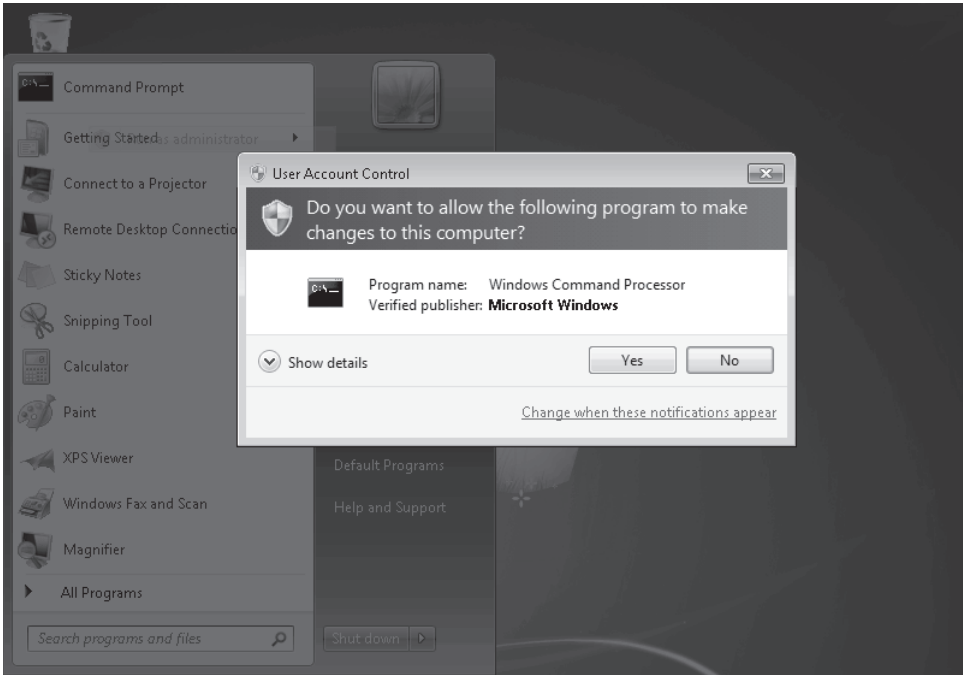

FIGURE 5-2 By default, UAC displays a consent prompt on a Secure Desktop to administrators who request to run a program with elevation.

Understanding UAC Notifications for Standard Users

The UAC notifications shown to standard users are distinct from those shown to administrators in that the notifications for standard users prompt these users to provide administrator credentials. As with administrators, standard users by default receive UAC notifications when they attempt to run a program such as a command prompt at elevated privileges, or when a program independently requests elevation. In addition, standard users by default receive UAC notifications when they attempt to make changes on the system that require administrator privileges. For example, if standard users open the System page in Control Panel and click Remote Settings, they see the credential prompt shown in Figure 5-3.

NOTE **THE DEFAULT BEHAVIOR OF UAC IS THE SAME FOR STANDARD USERS IN WINDOWS 7**

Although UAC in Windows 7 offers many notification levels that did not exist in Windows Vista or Windows Server 2008, the default behavior for standard users is the same. Whenever standard users attempt to make a change that requires administrator privileges, a credential prompt appears on a Secure Desktop.

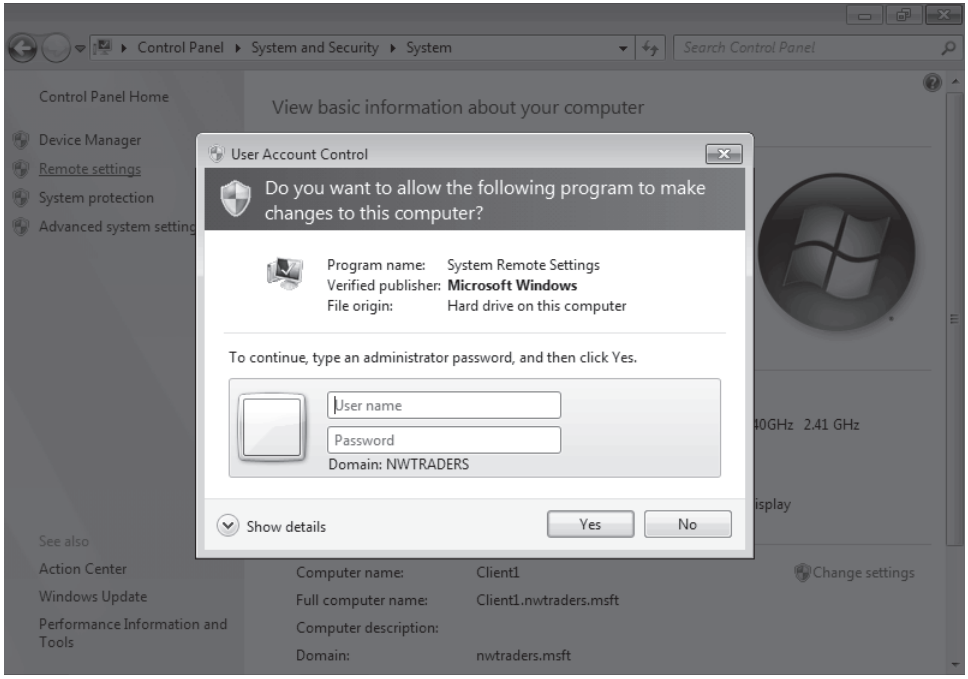

FIGURE 5-3 By default, UAC displays a credential prompt on a Secure Desktop to standard users who request elevation.

Configuring UAC in Control Panel

In a domain environment, it is recommended that UAC be controlled centrally by Group Policy instead of by configuration settings on each local machine. However, in workgroup environments or in domain environments in which Group Policy allows local UAC configuration, you can configure UAC through Control Panel.

To configure UAC in Control Panel, perform the following steps:

1. In Control Panel, click System and Security.
2. Under Action Center, click Change User Account Control Settings, as shown in Figure 5-4.

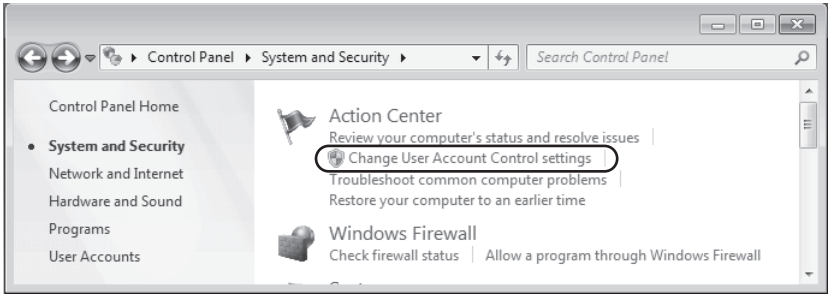

FIGURE 5-4 You can access UAC settings through the Action Center.

This step opens the User Account Settings window, one version of which is shown in Figure 5-5. Note that the set of options that appears is different for administrators and standard users, and that each user type has a different default setting.

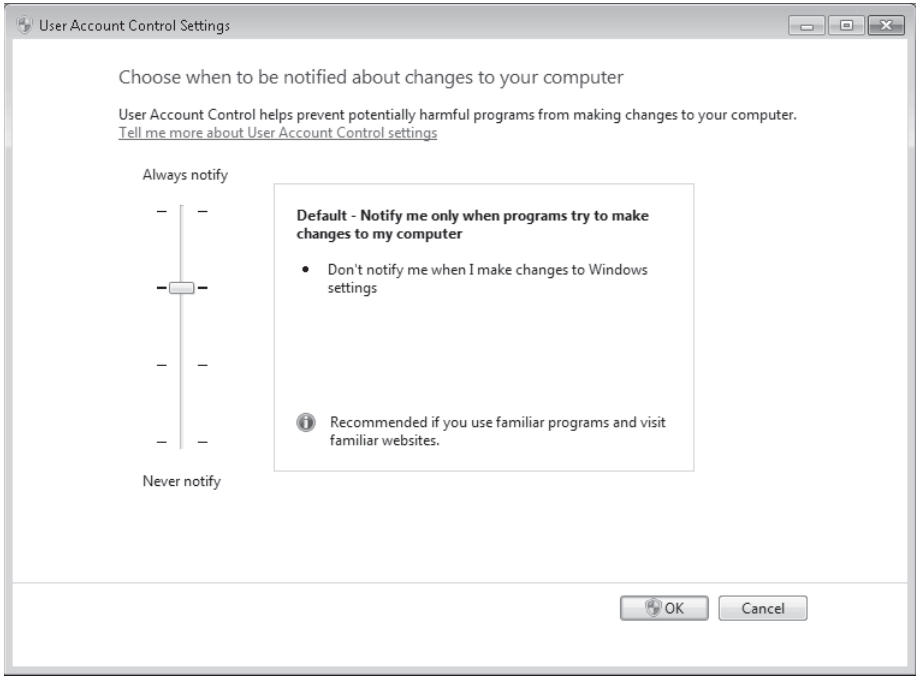

FIGURE 5-5 UAC allows you to choose among four notification levels.

3. Choose one of the following notification levels:
   - **Always Notify** This level is the default for standard users, and it configures UAC to act as it does in Windows Vista. At this level, users are notified whenever any changes that require administrator privileges are attempted on the system.
   - **Notify Me Only When Programs Try To Make Changes To My Computer** This level is the default for administrators and is not available for standard users. At this level, administrators are not notified when they make changes that require administrator privileges. However, users are notified through a consent prompt when a program requests elevation.
   - **Always Notify Me (And Do Not Dim My Desktop)** This level is not available for administrators. It is similar to the default setting for standard users, except that at this particular level, the Secure Desktop is never displayed. Disabling the Secure Desktop tends to reduce protection against malware, but it improves the user experience. This setting might be suitable for standard users who very frequently need to request elevation.

- **Notify Me Only When Programs Try To Make Changes To My Computer (Do Not Dim The Desktop)** This level is available for both standard users and administrators. At this level, the behavior is the same as with the default administrator level ("Notify me only when programs try to make changes to my computer"), but with this option the Secure Desktop is not displayed.
- **Never Notify** This level disables notifications in UAC. Users are not notified of any changes made to Windows settings or when software is installed. This option is appropriate only when you need to use programs that are incompatible with UAC.

4. Click OK.

Configuring UAC Through Group Policy

You can configure UAC through Local Security Policy or Group Policy settings. To find UAC-related policy settings in a GPO, navigate to the following node:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options

This location is shown in Figure 5-6.

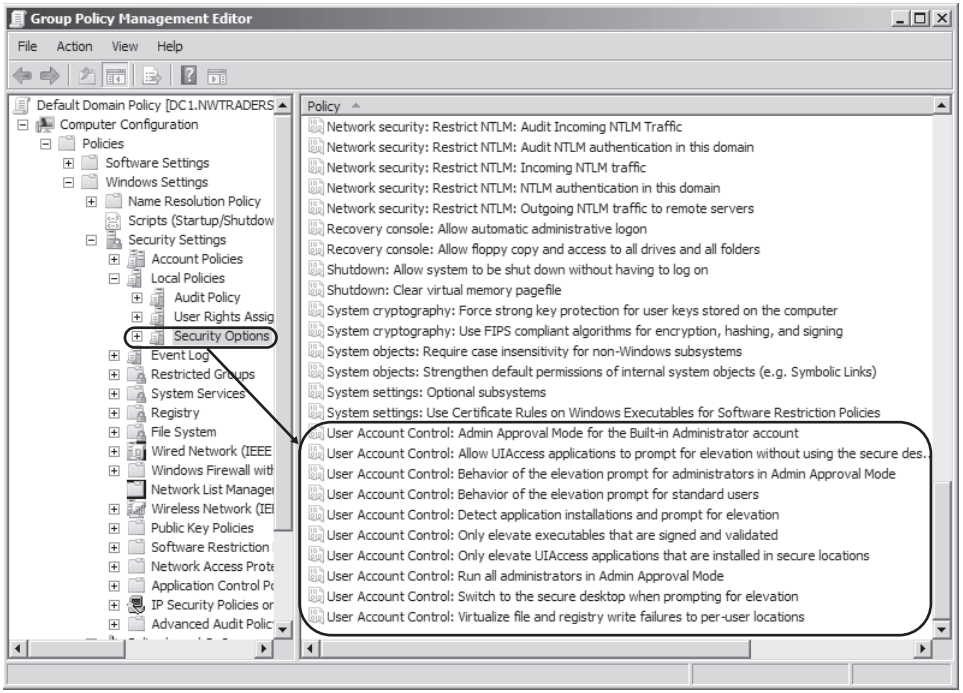

FIGURE 5-6 You can find UAC settings in Security Options in a GPO or in Local Security Policy

The following 10 UAC-related policy settings are available. The next section describes each of these configurable settings.

- **User Account Control: Admin Approval Mode For The Built-in Administrator Account** This policy applies only to the built-in Administrator account, and not to other accounts that are members of the local Administrators group. When you enable this policy setting, the built-in Administrator account sees UAC notifications just as other administrative accounts do. When you disable the setting, the built-in Administrator account behaves just like it does in Windows XP, and all processes run using Administrator privileges. This setting is disabled in Local Security Policy by default.
- **User Account Control: Allow UIAccess Applications to Prompt For Elevation Without Using The Secure Desktop** This setting controls whether user Interface Accessibility (UIAccess) programs can disable the Secure Desktop automatically. When enabled, UIAccess applications (such as Remote Assistance) automatically disable the Secure Desktop for elevation prompts. Disabling the Secure Desktop causes elevation prompts to appear on the standard desktop. By default, this setting is disabled in Local Security Policy.
- **User Account Control: Behavior Of The Elevation Prompt For Administrators In Admin Approval Mode** This policy setting controls the behavior of the elevation prompt for administrators. Six options are available:
  - **Elevate Without Prompting** With this option, administrators never see elevation prompts.
  - **Prompt For Credentials On The Secure Desktop** When this option is chosen, administrators see credential prompts on a Secure Desktop when elevation is requested.
  - **Prompt For Consent On The Secure Desktop** With this option, administrators see a consent prompt on a Secure Desktop when elevation is requested.
  - **Prompt For Credentials** When this option is selected, administrators see a credential prompt on a normal desktop when elevation is requested.
  - **Prompt For Consent** When this option is selected, administrators see a consent prompt on a normal desktop when elevation is requested.
  - **Prompt For Consent For Non-Windows Binaries** This option is the default setting in Local Security Policy. It causes a consent prompt to appear any time an application requests elevation.
- **User Account Control: Behavior Of The Elevation Prompt For Standard Users** This policy setting controls the behavior of the elevation prompt for standard users. Three options are available:
  - **Automatically Deny Elevation Requests** When this option is enforced, standard users are not able to perform tasks that require elevation.
  - **Prompt For Credentials On The Secure Desktop** With this option (the default setting in Local Security Policy), standards users see a credential prompt on the Secure Desktop when elevation is requested.
  - **Prompt For Credentials** When this option is chosen, standard users see a credential prompt on the normal desktop whenever elevation is requested.

- **User Account Control: Detect Application Installations And Prompt For Elevation** When enabled, this policy setting configures UAC to prompt for administrative credentials when the user attempts to install an application that makes changes to protected aspects of the system. When disabled, the prompt won't appear. Domain environments that use delegated installation technologies such as Group Policy Software Install (GPSI) or Microsoft Systems Management Server (SMS) can disable this feature safely because installation processes can escalate privileges automatically without user intervention. By default, this setting is enabled in Local Security Policy.
- **User Account Control: Only Elevate Executables That Are Signed And Validated** When this policy setting is enabled, Windows 7 refuses to run any executable that isn't signed with a trusted certificate, such as a certificate generated by an internal Public Key Infrastructure (PKI). When disabled, this policy setting allows users to run any executable, potentially including malware. If your environment requires all applications to be signed and validated with a trusted certificate, including internally developed applications, you can enable this policy to increase security greatly in your organization. This setting is disabled in Local Security Policy by default.
- **User Account Control: Only Elevate UIAccess Applications That Are Installed In Secure Locations** When enabled, this policy setting causes Windows 7 to grant user interface access only to those applications that are started from Program Files or subfolders, from Program Files (x86) or subfolders, or from \Windows\System32\. When disabled, the policy setting grants user interface access to applications regardless of where they are started in the file structure. This policy setting is enabled by default in Local Security Policy.
- **User Account Control: Run All Administrators In Admin Approval Mode** This policy setting, enabled by default in Local Security Policy, causes all accounts with administrator privileges *except* for the local Administrator account to see consent prompts when elevation is requested. If you disable this setting, administrators never see consent prompts and the Security Center displays a warning message.
- **User Account Control: Switch To The Secure Desktop When Prompting For Elevation** The Secure Desktop is a feature that darkens the screen and freezes all activity except for the UAC prompt. It reduces the possibility that malware can function, but some users might find that the feature slows down their work too much. When enabled, this policy setting causes the Secure Desktop to appear with a UAC prompt. When disabled, this policy setting allows UAC prompts to appear on a normal desktop. This policy setting is enabled by default in Local Security Policy.
- **User Account Control: Virtualize File And Registry Write Failures To Per-User Locations** This policy setting, enabled by default in Local Security Policy, improves compatibility with applications not developed for UAC by redirecting requests for protected resources. When disabled, this policy setting allows applications not developed for UAC to fail.

Disabling UAC Through Local or Group Policy

To force UAC to a disabled state, you can use Local Security Policy or Group Policy. First, set the User Account Control: Behavior Of The Elevation Prompt For Administrator In Admin Approval Mode setting to Elevate Without Prompting. Then, disable the User Account Control: Detect Application Installations And Prompt For Elevation and User Account Control: Run All Administrators In Admin Approval Mode settings. Finally, set User Account Control: Behavior Of The Elevation Prompt For Standard Users setting to Automatically Deny Elevation Requests. Then, restart the computers on which you want to apply the new settings.

Best Practices for Using UAC

To receive the security benefits of UAC while minimizing the costs, follow these best practices:

- Leave UAC enabled for client computers in your organization.
- Have all users—especially IT staff—log on with standard user privileges.
- Each user should have a single account with only standard user privileges. Do not give standard domain users accounts with administrator privileges to their local computers.
- Domain administrators should have two accounts: a standard user account that they use to log on to their computers, and a second administrator account that they can use to elevate privileges.
- Train users *not* to approve a UAC prompt if it appears unexpectedly. UAC prompts should appear only when the user is installing an application or starting a tool that requires elevated privileges. A UAC prompt that appears at any other time might have been initiated by malware. Rejecting the prompt helps prevent malware from making permanent changes to the computer.

Quick Check

- **Which Group Policy setting could you enable to prevent executables from running if they aren't signed with a trusted certificate?**

Quick Check Answer

- **User Account Control: Only Elevate Executables That Are Signed And Validated**

Whereas UAC is a set of features that broadly aims to protect core areas of the operating system, another Windows 7 tool—Windows Defender—has a much narrower goal of detecting and removing unwanted software.

Protecting Clients from Spyware with Windows Defender

Windows Defender is a tool in Windows 7 whose purpose is to detect and remove spyware on a client system. By default, Windows Defender is configured to download new spyware definitions regularly through Windows Update and then use these definitions to scan for

spyware on the local system. Often, you do not need to change this default configuration, though in large networks you might want to disable some Windows Defender features through Group Policy.

> ***NOTE*** **USE WINDOWS DEFENDER IN SMALL NETWORKS**
>
> **Windows Defender is a basic anti-malware program that is suitable for use in small networks or as a temporary solution before an advanced anti-malware solution is purchased. In large networks, you should use a centrally managed anti-malware solution such as Microsoft Forefront Client Security.**

To view Windows Defender, open Control Panel, select View By Large Icons, and then scroll down to click Windows Defender, as shown in Figure 5-7. (Alternatively, you can click Start, type **windows defender**, and select Windows Defender in the Start menu.)

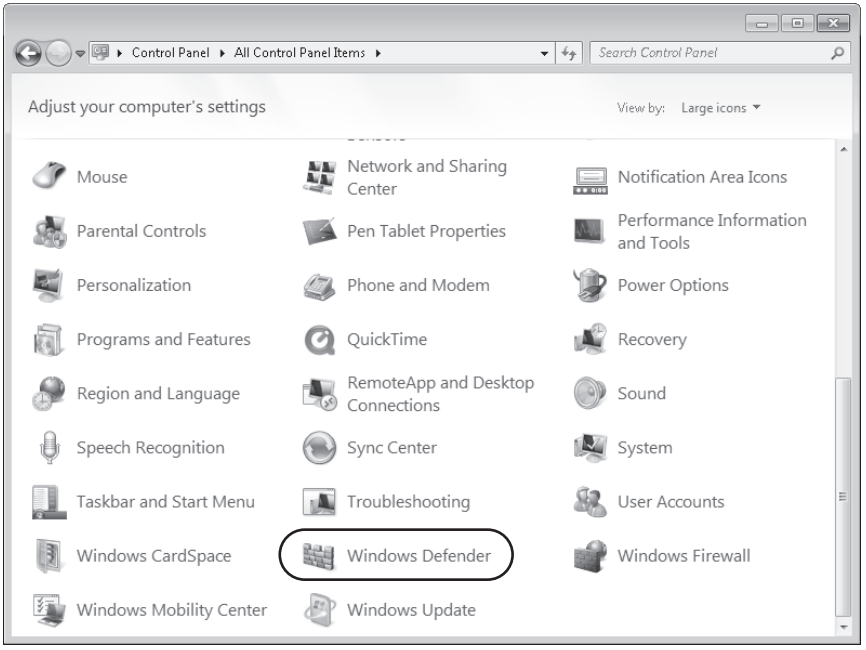

FIGURE 5-7 Opening Windows Defender

Windows Defender is shown in Figure 5-8.

By default, Windows Defender provides two types of protection:

- **Automatic scanning** Windows Defender is configured by default to download new definitions and then perform a quick scan for spyware at 2 A.M. daily.
- **Real-time protection** With this feature, Windows Defender constantly monitors computer usage in areas such as the Startup folder, the Run keys in the registry, and Windows add-ons. If an application attempts to make a change to one of these areas, Windows Defender prompts the user either to Permit (allow) or Deny (block) the change.

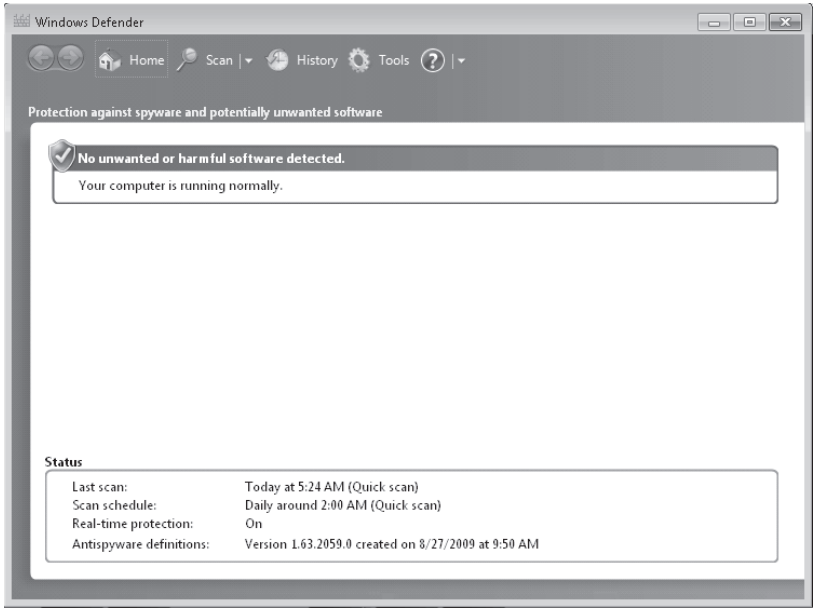

FIGURE 5-8 Windows Defender automatically checking for spyware

Besides providing this automatic functionality, Windows Defender also lets you perform a manual scan of the system. You can start a manual scan by selecting Quick Scan, Full Scan, or Custom Scan from the Scan menu, as shown in Figure 5-9.

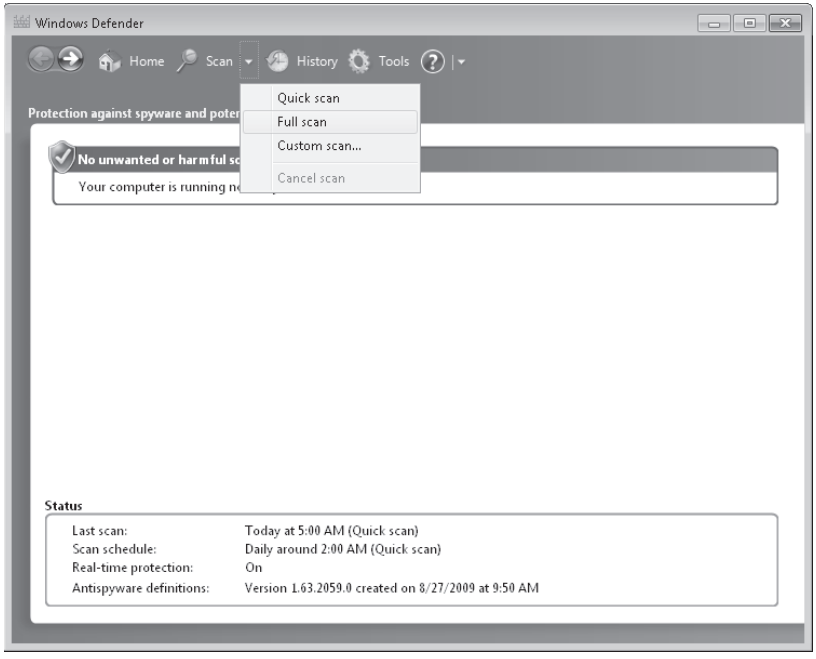

FIGURE 5-9 Performing a manual scan in Windows Defender

These three scan types are described in the following list:

- **Quick Scan** This type of scan scans only the areas of a computer most likely to be infected by spyware or other potentially unwanted software. These areas include the computer's memory and portions of the registry that link to startup applications. A quick scan is sufficient to detect most spyware.
- **Full Scan** This type of scan scans every file on the computer, including common types of file archives and applications already loaded in the computer's memory. A full scan typically takes several hours and can even take more than a day. You need to run a full scan only if you suspect that a user's computer is infected with unwanted software after the quick scan is run.
- **Custom Scan** Custom scans begin with a quick scan and then perform a detailed scan on the specific portions of a computer that you choose.

NOTE **YOU CAN WORK ON A COMPUTER WHILE A SCAN IS IN PROGRESS**

Although scans slow the computer down, a user can continue to work on the computer while a scan is in progress. Note also that scans consume battery power on mobile computers very quickly.

Handling Detected Spyware

If Windows Defender finds spyware or potentially unwanted software as a result of a scan, it displays a warning and provides you with four options for each item detected:

- **Ignore** This option allows the detected software to remain untouched on your computer and stay detectable by Windows Defender whenever the next scan is performed. This option might be appropriate when you need to research the software that Windows Defender has found before you decide to remove it.
- **Quarantine** This option isolates the detected software. When Windows Defender quarantines software, it moves it to another location on your computer and then prevents the software from running until you choose to restore it or remove it from your computer. This option is used most often when the detected software cannot be removed successfully.
- **Remove** This option deletes the detected software from your computer. You should choose this option unless you have a compelling reason not to.
- **Always Allow** The option adds the software to the Windows Defender Allowed list and allows it to run on your computer. Windows Defender stops alerting you to actions taken by the program. You should choose this option only if you trust the software and the software publisher.

Configuring Windows Defender Through Group Policy

In an AD DS environment, it is recommended that you configure clients by using Group Policy instead of individually on each machine. To find the Group Policy settings for Windows Defender, open a GPO and navigate to Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender, as shown in Figure 5-10.

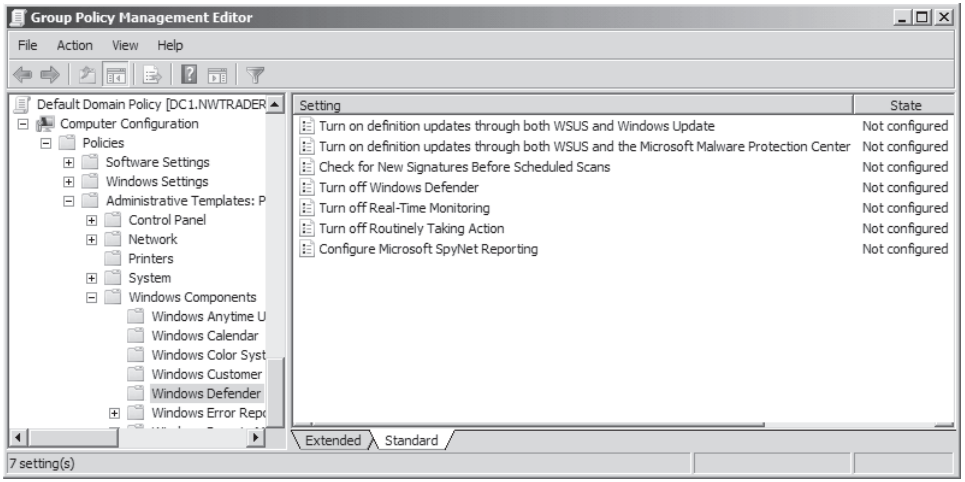

FIGURE 5-10 Group Policy settings for Windows Defender

The following seven policy settings for Windows Defender are available:

- **Turn On Definition Updates Through Both WSUS And Windows Update** If you enable or do not configure this policy setting and the Automatic Updates client is configured to point to a WSUS server, Windows Defender obtains definition updates from Windows Update if connections to that WSUS server fail. If you disable this setting, Windows Defender checks for updates only according to the setting defined for the Automatic Updates client—either by using an internal WSUS server or Windows Update.
- **Turn On Definition Updates Through Both WSUS And The Microsoft Malware Protection Center** If you enable or do not configure this policy setting and the Automatic Updates client is configured to point to a WSUS server, Windows Defender checks for definition updates from both WSUS and the Microsoft Malware Protection Center if connections to that WSUS server fail. If you disable this setting, Windows Defender checks for updates only according to the setting defined for the Automatic Updates client—either by using an internal WSUS server or Windows Update.
- **Check For New Signatures Before Scheduled Scans** If you enable this policy setting, Windows Defender always checks for new definitions before it begins a scheduled scan of the computer. When you disable or do not configure this setting, Windows Defender does not check for new definitions immediately before beginning scheduled scans.

- **Turn Off Windows Defender** If you enable this policy setting, Windows Defender no longer performs any real-time or scheduled scans. (However, users can still perform manual scans.) You should enable this setting if you have implemented a more advanced anti-spyware solution such as Microsoft Forefront Client Security. If you disable or do not configure this policy setting, Windows Defender performs both real-time scans and any scheduled scans.
- **Turn Off Real-Time Monitoring** If you enable this policy setting, Windows Defender does not automatically prompt users to allow or block activity in protected areas of the operating system. If you disable or do not configure this policy setting, by default Windows Defender prompts users to allow or block potential spyware activity on their computers.
- **Turn Off Routinely Taking Action** If you enable this policy setting, Windows Defender only prompts the user to choose how to respond to a threat but not to take any automatic action. If you disable or do not configure this policy setting, Windows Defender automatically takes action on detected threats after approximately 10 minutes.
- **Configure Microsoft SpyNet Reporting** SpyNet is an online community that pools information about threats experienced by its members. SpyNet learns from the user responses to these threats to determine which threats are benign and which are malicious.

  If you enable this policy setting and choose the "No Membership" option, SpyNet membership is disabled, and no information is sent to Microsoft. If you enable this policy setting and choose the "Advanced" option, SpyNet membership is set to Advanced, and information about detected threats and the responses to those threats is sent to Microsoft.

  If you disable or do not configure this policy setting, SpyNet membership is disabled by default, but local users can change the membership setting.

NOTE **USING A BOOTABLE ANTIVIRUS CD**

When a computer has become severely infected with malware, the computer might run so slowly that it's difficult to perform an anti-malware scan. In this case, it's a good idea to perform an offline scan from a bootable CD if you have one available. By performing the scan outside of Windows, you avoid running the malware programs that consume resources and slow down the system.

Best Practices for Using Windows Defender

To receive the security benefits of Windows Defender while minimizing the costs, follow these best practices:

- Before deploying Windows 7, test all applications with Windows Defender enabled to ensure that Windows Defender does not alert users to normal changes that the application might make. If a legitimate application does cause warnings, add the application to the Windows Defender Allowed list.

- Change the scheduled scan time to meet the needs of your business. By default, Windows Defender scans at 2 A.M. If third-shift staff uses computers overnight, you might want to find a better time to perform the scan. If users turn off their computers when they are not in the office, you should schedule the scan to occur during the day.
- Use WSUS to manage and distribute signature updates.
- Use antivirus software with Windows Defender. Alternatively, you might disable Windows Defender completely and use client-security software that provides both anti-spyware and antivirus functionality.
- Do not deploy Windows Defender in large enterprises. Instead, use Forefront or a third-party client-security suite that can be managed more easily in enterprise environments.

MORE INFO **WINDOWS DEFENDER**

For more information about Windows Defender, visit the Windows Defender Virtual Lab Express at *http://www.microsoftvirtuallabs.com/express/registration.aspx?LabId=92e04589-cdd9-4e69-8b1b-2d131d9037af*.

Determining When Your System Is Infected with Malware

As a enterprise support technician, you need to know how to recognize the symptoms of a malware infection on your client computers. Then, if your antivirus and anti-spyware are not functioning or not detecting any malware, you need to know how to remove malware manually.

Here are a few common signs of a computer being infected by a virus, worm, or Trojan horse:

- Sluggish computer performance
- Unusual error messages
- Distorted menus and dialog boxes
- Antivirus software repeatedly turning itself off
- Screen freezing
- Computer crashing
- Computer restarting
- Applications not functioning correctly
- Inaccessible disk drives, or a CD-ROM drive that automatically opens and closes
- Notification messages that an application has attempted to contact you from the Internet
- Unusual audio sounds
- Printing problems

Note that, although these are common signs of infection, these symptoms might also indicate other types of hardware or software problems that are unrelated to malware.

Signs of a spyware infection tend to be slightly different from those of other types of malware. If you see any of the following symptoms, suspect spyware:

- A new, unexpected application appears.
- Unexpected icons appear in the system tray.
- Unexpected notifications appear near the system tray.
- The Web browser home page, default search engine, or favorites change.
- New toolbars appear, especially in Web browsers.
- The mouse pointer changes.
- The Web browser displays additional advertisements when visiting a Web page, or pop-up advertisements appear when the user is not using the Web.
- When the user attempts to visit a Web page, she is redirected to a completely different Web page.
- The computer runs more slowly than usual.

Some spyware might not have any noticeable symptoms, but it still might compromise private information.

How to Resolve Malware Infections

The most important way to resolve malware infections is to prevent them in the first place by running antivirus and anti-spyware programs daily with the latest virus and spyware definitions. If malware is discovered on a system, use the application to remove the malware if possible and quarantine it if not. If it is a new malware program, you might need to run a removal tool or perform a series of steps to remove it manually.

These steps naturally apply to malware that is detected. However, as important as it is to remember to use antivirus and anti-spyware daily, it is just as important to remember that no anti-malware application is foolproof. Many malware programs are in fact written around anti-malware software so that they cannot be detected. And if even a single malicious feature remains after a scan, that remaining malware program can install other malware programs.

If you suspect a problem related to malware after running antivirus and anti-spyware applications with the latest definitions, take the following steps:

1. If you notice changes to Windows Internet Explorer, such as unwanted add-ons or a new home page, use Control Panel to look for and uninstall any unnecessary programs.
2. Use the Startup tab of the System Configuration utility (Msconfig.exe) to clear any unnecessary startup programs. Note the Registry entry associated with any of these programs. (You can use this Registry information to delete the associated Registry keys if necessary.) Use the Services tab to disable any unnecessary services.

3. Open Task Manager. Note any unusual services listed on the Services tab or unusual processes listed on the Processes tab. (Be sure to click Show Processes From All Users so you can see all running processes.) Use the Go To Process option on the Services tab and the Go To Service(s) option on the Processes tab to help learn the connection between services and processes that are unknown to you. Then, perform Web searches on services and processes that lack descriptions or that otherwise seem suspicious. If you can determine from your research that any services or processes are associated with malware, right-click them to stop them. Then, in the Services console, disable the associated service so that it cannot run again.
4. Open the Registry Editor (Regedit.exe). Navigate to HKLM\Software\Microsoft\Windows\CurrentVersion\Run. In the details pane, note any Registry values associated with unwanted started programs. Write the path names provided to the target files in the Data column, as shown in Figure 5-11, and then delete the Registry values. Then, navigate to HKCU\Software\Microsoft\Windows\CurrentVersion\Run and do the same.

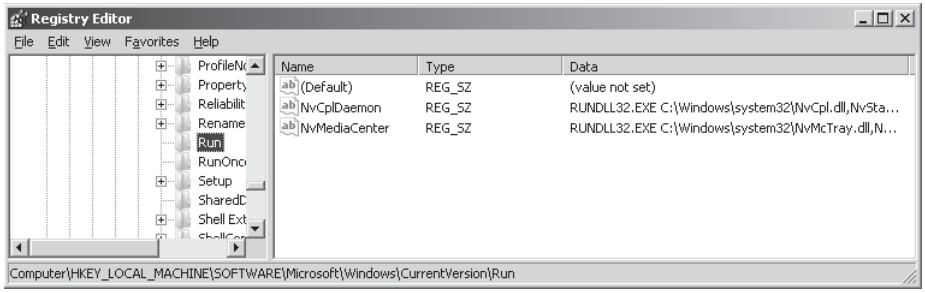

FIGURE 5-11 Copy down the path names to files associated with unwanted startup programs, and then delete the Registry values.

5. Using the path name information that you copied in step 4, visit these locations in the Windows file structure and delete the target files.
6. If you still see signs of malware, install an additional anti-spyware and antivirus application from a known and trusted vendor. Your chances of removing all traces of malware increase by using multiple applications, but you should not configure multiple applications to provide real-time protection.
7. If problems persist, shut down the computer and use the Startup Repair tool to perform a System Restore. Restore the computer to a date prior to the malware infection. System Restore typically removes any startup settings that cause malware applications to run, but it does not remove the executable files themselves. Do this only as a last resort: Although System Restore does not remove a user's personal files, it can cause problems with recently installed or configured applications.

Performing this series of steps resolves a great majority of malware problems. However, once malware has run on a computer, you can never be certain that the software is removed completely. In particular, rootkits are difficult to detect and remove. In these circumstances, if you suspect a rootkit and cannot remove it, you might be forced to reformat the hard disk, reinstall Windows, and then restore user files using a backup created prior to the infection.

PRACTICE Enforcing an Anti-Malware Policy Through Group Policy

In this practice, you use Group Policy to enforce specific settings for UAC and Windows Defender. These exercises require a domain controller running Windows Server 2008 R2 and a client running Windows 7 that is a member of the same domain.

EXERCISE 1 Enforcing UAC Settings Through Group Policy

In this exercise, you enforce new UAC default settings on computers running Windows 7 in the domain.

1. Log on to the domain controller.
2. Open Group Policy Management by clicking Start\All Programs\Administrative Tools\Group Policy Management.
3. In the Group Policy Management console tree, navigate to Group Policy Management\Forest: *Forest Name*\Domains*Domain Name*\Default Domain Policy.
4. Right-click Default Domain Policy, and then click Edit from the shortcut menu. The Group Policy Management Editor opens.
5. In the Group Policy Management Editor, navigate to Default Domain Policy\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options.
6. In the details pane, double-click to open User Account Control: Switch To The Secure Desktop When Prompting For Elevation.
7. On the Security Settings tab, click Define This Policy Setting, select Disabled, and then Click OK.
8. In the details pane, double-click to open User Account Control: Behavior Of The Elevation Prompt For Standard Users.
9. On the Security Settings tab, click Define This Policy Setting, select Prompt For Credentials from the drop-down list, and then Click OK.

   These settings remove the Secure Desktop from all UAC prompts.
10. Click OK.
11. Switch to the client running Windows 7. Restart the client, and then log on to the domain from the client as a domain administrator.
12. Open an elevated command prompt by clicking Start\All Programs\Accessories, then right-clicking Command Prompt and clicking Run As Administrator from the shortcut menu.
13. A consent prompt appears without a Secure Desktop.
14. Log off the client, and then log on again to the domain from the client as a standard user without administrative privileges.
15. In Control Panel, beneath User Accounts, click Change Account Type. A credential prompt appears without a Secure Desktop.
16. Log off the client.

EXERCISE 2 Disabling Real-Time Monitoring for Windows Defender

A large corporate network should use a managed anti-spyware solution, which Windows Defender is not. Using Windows Defender to provide a secondary daily scan for malware on clients is a good idea, but you should not have two applications performing real-time monitoring. If your managed anti-spyware solution provides real-time monitoring, you should disable the same feature on Windows Defender by using Group Policy.

In this exercise, you use Group Policy to disable real-time monitoring for Windows Defender.

1. Log on to the domain controller.
2. Using the steps described in Exercise 1, open Group Policy Management and then choose to edit the Default Domain Policy.
3. In the Group Policy Management Editor, navigate to Default Domain Policy\Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender.
4. In the details pane, double-click to open Turn Off Real-Time Monitoring.
5. In the Turn Off Real-Time Monitoring dialog box, select Enabled, and then click OK.
6. Switch to Client1. Log on to the domain from Client1 as a domain administrator.
7. Open a command prompt and type **gpupdate**. You might see a notification bubble appear indicating that Windows Defender is turned off.
8. After the command finishes executing, click Start, type **windows defender**, and then click Windows Defender in the Start menu.
9. In Windows Defender, click Tools, and then click Options.
10. Select Real-Time Protection from the list of options.
11. The settings are dimmed. Real-time monitoring is disabled.
12. Return to the domain controller and the Default Domain Policy. Revert the Turn Off Real-Time Monitoring policy setting to Not Configured, and then click OK.
13. Rerun **gpupdate** on Client1, and then close all open windows on both computers.

Lesson Summary

- UAC helps prevent malware from secretly installing itself on Windows systems by notifying the user whenever a request is made to write to protected areas of the operating system. Users must be educated to dismiss these notifications if they have not initiated them.
- You can configure the behavior of UAC notifications. By default, administrators see consent prompts on a Secure Desktop when a program requests elevation. Standard users by default see credential prompts on a Secure Desktop whenever they or a program requests elevation.

- Windows Defender is a built-in feature of Windows 7 that provides basic spyware filtering and detection. Often Windows Defender needs no configuration, but you might want to disable it in larger networks that require a managed anti-spyware solution.
- You should how to check for and remove malware manually in case your anti-malware solution isn't functioning as desired. To do so, investigate unknown processes and services to stop and disable them if necessary, and look in the Registry for programs that are set to run automatically. Delete associated files.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Resolving Malware Issues." The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE*** **ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.**

1. You work as an enterprise support technician in a large company. Your manager reports that some network administrators are using the built-in Administrator account for the domain and that, when logged on with this account, they are not seeing UAC notifications. She asks you to change configuration settings so that users logged on to the domain with the built-in Administrator account see UAC consent prompts. What should you do?
   - **A.** Configure Local Security Policy to set the User Account Control: Admin Approval Mode For The Built-in Administrator Account option to Enabled.
   - **B.** Configure Group Policy to set the User Account Control: Admin Approval Mode For The Built-in Administrator Account option to Enabled.
   - **C.** Configure Local Security Policy to set the User Account Control: Run All Administrators In Admin Approval Mode option to Enabled.
   - **D.** Configure Group Policy to set the User Account Control: Run All Administrators In Admin Approval Mode option to Enabled.
2. You work as an enterprise support technician in a company whose AD DS domain consists of 20 servers running Windows Server 2008 R2 and 500 client computers running Windows 7, 10 of which are portable and are used by employees who travel globally for work. These users have complained that Windows Defender tends to start a scan when the computer is operating on the battery source, and the scan quickly

consumes battery power. You want to prevent Windows Defender from consuming needed battery power without reducing the protection that it provides. What should you do?

A. Instruct the users to perform a manual scan when their computers are connected to a power source.

B. Choose the option to run a scan only when idle.

C. Instruct the users to adjust the schedule for automatic scanning.

D. Disable automatic scanning on all 10 computers.

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenario. The scenario sets up a real-world situation involving the topics of this chapter and asks you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- Windows Firewall blocks all incoming connection requests by default. To allow a network program to initiate a connection with a computer running Windows 7, you need to create a firewall exception for that program.
- To combat malware, you need to educate yourself and users continually about the evolving nature of threats. You also need to manage antivirus software, anti-spyware software such as Windows Defender, and UAC effectively. Finally, you need to know how to recognize classic symptoms of an infection and how to remove an infection manually if needed.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- **Exception**
- **Malware**
- **Spyware**
- **Virus**
- **Worm**

Case Scenario

In the following case scenario, you apply what you've learned about protecting client systems. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Resolving Malware Infections

You work as an enterprise support technician for Contoso, Ltd., a marketing research firm with 500 employees. You receive a call from the help desk to investigate a research assistant's notebook computer that is apparently running very slowly. A help desk support technician was unable to resolve the issue.

You perform some basic testing on the computer, and you discover that several toolbars associated with spyware are installed in Internet Explorer. Your company uses a combined antivirus/anti-spyware solution, and Windows Defender is disabled on the network.

You conduct interviews with the Research Assistant and the Help Desk Support Technician.

Interviews

The following is a list of company personnel interviewed and their statements:

- **Research Assistant** "The problem has been getting progressively worse for about six months. It's gotten to the point that everything takes forever. I used to take this computer home with me, but now I don't even bother."
- **Help Desk Support Technician** "I tried to run an anti-malware scan, but nothing seemed to happen."

Questions

1. You want to immediately stop any malware that might be running. How should you achieve this?
2. Your testing reveals that the anti-malware client software installed on the computer does not run when it is opened. What can you do to perform an anti-malware scan on the computer?

Suggested Practices

To help you master the exam objectives presented in this chapter, complete the following tasks.

Identify and Resolve Issues Due to Malicious Software

Perform these practices to learn about tools that help detect and remove malware.

- **Practice 1** Perform a Web search for the term "Sysinternals Suite" or visit *http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx*. Download the Sysinternals Suite and unzip the file. Within the suite, locate Autoruns. Run Autoruns to discover the programs that are configured to start up automatically on your computer. Then, locate and run Rootkitrevealer to discover any rootkits on your system.

- **Practice 2** Perform a Web search for the term "bootable anti-malware CD" and research the various bootable anti-malware CDs that are available online. Create or download a bootable anti-malware CD and then use it to perform a malware scan on your system.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-685 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **PRACTICE TESTS**

For details about all the practice test options available, see the section entitled "How to Use the Practice Tests," in the Introduction to this book.

CHAPTER 8

Performance

Windows 7 should be the best performing version of Windows ever. However, all computers have limited processor, memory, and disk resources, and any computer will respond slowly under the right circumstances. Because you can't create a completely problem-free IT environment, you must plan to identify and resolve performance problems quickly when they do occur. Windows 7 includes several features that enable administrators to monitor and respond to performance problems.

First, Windows 7 can forward events between computers, enabling you to collect significant events centrally from across your network. With Task Manager, you can monitor performance in real time, adjust priorities and affinities of different processes to control how much processor time they consume, and end processes that are not responding to user input. Performance Monitor provides even more in-depth information about system performance, enabling you to monitor minute details of the operating system, applications, and hardware.

For performance problems that are short-lived, you can create a snapshot of system performance information using a data collector set and then analyze the performance information at your leisure. If you identify the hard disk as a source of your performance problems, you might need to free up some disk space using the Disk Cleanup tool so that Windows 7 can defragment the disk automatically.

Performance for mobile computers is more complex than desktop computers, because they typically have performance settings to optimize battery usage. To troubleshoot performance issues with mobile computers properly, you must understand how to configure the different performance settings. Finally, if a performance problem seems to be caused by a startup service or application, you can use the System Configuration tool to disable different startup services and applications temporarily to allow you to identify the source of the problem.

Exam objective in this chapter:

- Identify and resolve performance issues.

Lessons in this chapter:

Before You Begin

To complete the lessons in this chapter, you should be familiar with Windows 7 and be comfortable with the following tasks:

- Installing Windows 7
- Physically connecting a computer to a network
- Performing basic administration tasks on a Windows Server 2008 R2–based domain controller

REAL WORLD

Tony Northrup

Recently, I was troubleshooting intermittent performance problems with a Web server. At seemingly random times, the Web server would slow down to the point that users couldn't browse the site. By the time I received a complaint from a user, however, the site would already be back online.

To identify the problem, I ran Performance Monitor in logging mode. This allowed me to discover that, during the 10-minute period when users had problems, total processor utilization increased to 100 percent (when it was normally about 10 percent), and the time required to respond to Web requests went above 30 seconds (when it was normally about 0.02 seconds). While I monitored the performance of each individual process, none of the processes were consuming the extra processor time—meaning that the process wasn't running at the time I configured Performance Monitor. Performance Monitor had helped me identify more symptoms of the problem, but I still hadn't found the specific problem.

I made note of the time at which the problem occurred and checked that time range in Event Viewer. I found Web server errors messages indicating that Web requests had taken too long to process. That wasn't the source of the problem, though; it was just a secondary condition caused by the high processor utilization.

That event was the key to troubleshooting the problem further, however, because it occurred consistently when the problem began. I set up an event trigger to send a message to my phone whenever the event occurred. The next time it occurred, I ran to the Web server console, opened Task Manager, and identified the process that was consuming all the processor time.

The process was a script that cleaned up the database. The way the script was written, it would use 100 percent of the processor time, slowing down the entire server. The Web server automatically started the script after a specific number of database transactions, which explained why it seemed to occur randomly.

To resolve the problem, I changed the way the script was started. Instead of starting the script directly, I called the Start.exe tool, used the *//low* parameter to specify that the script run with a lower priority, and used the *//affinity* parameter to specify that the script use only one of the four processor cores on the Web server. The script took longer to run, but it no longer interfered with normal Web server activity.

Lesson 1: Forwarding Events

In Microsoft Windows, both the operating system and applications add events to event logs. Most of these events are informational (such as an event indicating that the computer is starting up) and can be safely ignored. However, very important events are often buried within thousands of insignificant events. These important events might indicate an impending hard disk failure, a security compromise, or a user who cannot access critical network resources.

Every computer running Windows has a local event log. Because enterprises often have thousands of computers, each with its own local event log, monitoring significant events was very difficult with earlier versions of Windows. *Event forwarding* in Windows Vista and Windows 7 makes it much easier for enterprises to manage local event logs. With event forwarding, you can configure computers running Windows to forward important events to a central location. You can then more easily monitor and respond to these centralized events.

This lesson describes how to configure and manage event forwarding.

After this lesson, you will be able to:

- Describe how event forwarding works.
- Configure event forwarding in Active Directory Domain Services (AD DS) environments.
- Configure event forwarding in workgroup environments.
- Troubleshoot event forwarding.

Estimated lesson time: 30 minutes

How Event Forwarding Works

Event forwarding uses Hypertext Transfer Protocol (HTTP) or HTTPS (Hypertext Transfer Protocol Secure), the same protocols used to browse Web sites, to send events from a *forwarding computer* (the computer that is generating the events) to a *collecting computer* (the computer that is configured to collect events). With event forwarding, you can send important events from any computer in your organization to your workstation, so that you can monitor the events from a central location.

Even though HTTP is normally unencrypted, event forwarding sends communications encrypted with the Microsoft Negotiate security support provider (SSP) in workgroup environments or the Microsoft Kerberos SSP in domain environments. HTTPS uses a Secure Sockets Layer (SSL) certificate (which you will need to generate) to provide an additional layer of encryption. This additional layer of encryption is unnecessary in most environments.

MORE INFO **MORE ABOUT SSP PROVIDERS**

For more information about SSP providers, read *http://msdn2.microsoft.com/en-us/library/aa380502.aspx*.

EXAM TIP

For the exam, remember that event forwarding uses encryption even if you choose the HTTP protocol. That's counterintuitive because when you use HTTP to browse the Web, it's always unencrypted.

How to Configure Event Forwarding in AD DS Domains

To forward events, you must configure both the forwarding and collecting computers. The forwarding computer is the computer that generates the events, and the collecting computer is the management workstation that administrators use to monitor events. The configuration you create for forwarding and collecting events is called an *event subscription*.

Event forwarding is not enabled by default on Windows 7. Before you can use event forwarding, both the forwarding and collecting computer must have two services running:

- Windows Remote Management
- Windows Event Collector

In addition, the forwarding computer must have a Windows Firewall exception for the HTTP protocol. Depending on the event delivery optimization technique you choose, you might also have to configure a Windows Firewall exception for the collecting computer. Fortunately, Windows 7 provides tools that automate the configuration of forwarding and collecting computers.

The sections that follow describe step by step how to configure computers for event forwarding.

How to Configure the Forwarding Computer

To configure a computer running Windows 7 to forward events, follow these steps on the forwarding computer:

1. Open a command prompt with administrative privileges by clicking Start, typing **cmd**, and pressing Ctrl+Shift+Enter.

TIP **OPENING AN ADMINISTRATIVE COMMAND PROMPT**

You can also open an administrative command prompt by right-clicking the command prompt in the Start menu and clicking Run As Administrator. Pressing Ctrl+Shift+Enter is just a shortcut to make the process quicker (especially for those who prefer to use the keyboard over the mouse).

2. At the command prompt, run the following command (shown in bold) to configure the Windows Remote Management service:

```
C:\>winrm quickconfig
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Set the WinRM service type to delayed auto start.
Start the WinRM service.

Make these changes [y/n]?
```

3. Type **Y**, and then press Enter. The Windows Remote Management service prompts you again:

```
WinRM has been updated to receive requests.

WinRM service type changed successfully.
WinRM service started.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this
machine.
Enable the WinRM firewall exception.

Make these changes [y/n]?
```

4. Type **Y**, and then press Enter. The Windows Remote Management service prompts you again.

   WinRm (the Windows Remote Management command-line tool) configures the computer to accept WS-Management requests from other computers. This involves making the following changes:

   - Sets the Windows Remote Management (WS-Management) service to Automatic (Delayed Start) and starts the service.
   - Configures a Windows Remote Management HTTP listener. A *listener* is a configuration setting that forwards specific incoming network communications to an application.
   - Creates a Windows Firewall exception to allow incoming connections to the Windows Remote Management service using HTTP on Transmission Control Protocol (TCP) port 80. This exception applies only to the Domain and Private profiles; traffic will still be blocked while the computer is connected to Public networks.

NOTE **AUTOMATIC (DELAYED START)**

Starting with Windows Vista, services could start with the Automatic (Delayed Start) startup type. Whereas Automatic services start as soon as Windows starts (slowing down the user logon), Automatic (Delayed Start) starts in the background, shortly after Windows starts. It's the perfect startup type for services that you need to have running but aren't critical to Windows functioning.

Next, you must add the computer account of the collector computer to the local Event Log Readers group on each of the forwarding computers by following these steps on the forwarding computer:

1. Click Start, right-click Computer, and then click Manage.
2. Under System Tools, expand Local Users And Groups, and then select Groups. Double-click Event Log Readers.
3. In the Event Log Readers Properties dialog box, click Add.
4. In the Select Users, Computers, Service Accounts, Or Groups dialog box, click Object Types. By default, it searches only users, service accounts, and groups. However, we need to add the collecting computer account. Select the Computers check box and clear the Groups, Users, and Service Accounts check boxes. Click OK.
5. In the Select Users, Computers, Or Groups dialog box, type the name of the collecting computer. Then, click OK.
6. Click OK again to close the Event Log Readers Properties dialog box.

Alternatively, you could perform this step from an elevated command prompt or a batch file by running the following command: *net localgroup "Event Log Readers" <computer_name>$@<domain_name> /add*.

For example, to add the computer WIN7 in the nwtraders.msft domain, you would run the following command: *net localgroup "Event Log Readers" win7$@nwtraders.msft /add*.

How to Configure the Collecting Computer

Windows 7 supports two types of event forwarding, which you specify when you create an event subscription:

- **Collector-initiated** In collector-initiated subscriptions, the collecting computer establishes a connection to the forwarding computer.
- **Source computer–initiated** In source computer–initiated subscriptions, the forwarding computer establishes a connection to the forwarding computer. Source computer–initiated subscriptions are the only subscription type available in workgroup environments.

If you plan to use collector-initiated subscriptions, Windows 7 prompts you to configure the collecting computer when you create a subscription, as described in the next section. Alternatively, you can preconfigure a collecting computer by performing these steps:

1. Open an elevated command prompt by clicking Start, typing **cmd**, and pressing Ctrl+Shift+Enter.
2. At the command prompt, run the following command to configure the Windows Event Collector service:

   ```
   wecutil qc
   ```

3. When prompted, press Y.

   Windows configures the Windows Event Collector service.

If you plan to use source computer–initiated subscriptions, you need to run *winrm quickconfig* on the collecting computer, as described in the section entitled "How to Configure the Forwarding Computer," earlier in this chapter.

Windows Server 2008 also includes the ability to collect forwarded events. However, versions of Windows released prior to Windows Vista do not support acting as a collecting computer or as a forwarding computer.

How to Create an Event Subscription

Subscriptions, as shown in Figure 8-1, are configured on a collecting computer and retrieve events from forwarding computers.

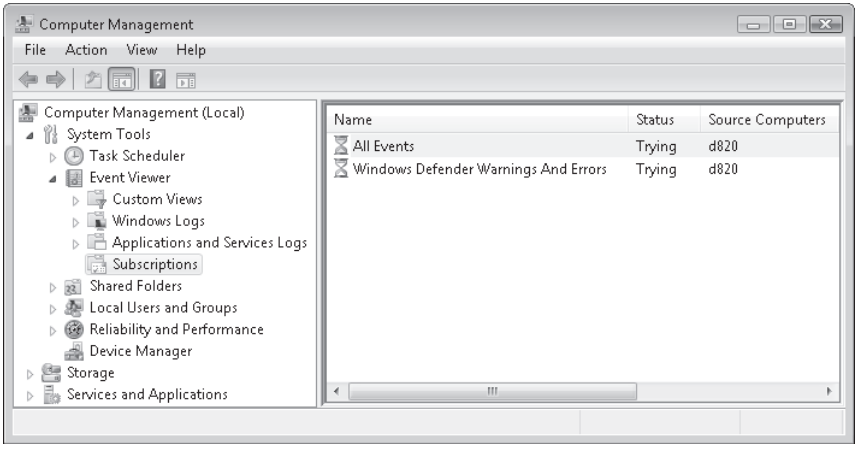

FIGURE 8-1 Subscriptions forward events to a management computer.

To create a subscription on a collecting computer, perform these steps:

1. In the Computer Management console, right-click Event Viewer\Subscriptions, and then click Create Subscription.

2. If prompted, click Yes to configure the Windows Event Collector service, as shown in Figure 8-2.

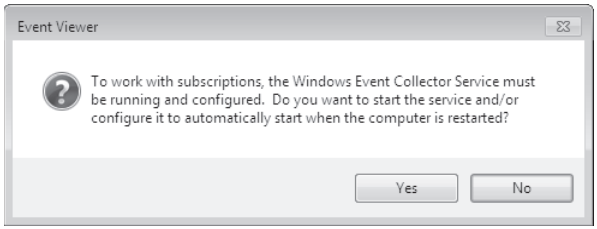

FIGURE 8-2 Pushing events from the forwarding computer to the collecting computer

The Subscription Properties dialog box appears.

3. In the Subscription Name box, type a name for the subscription, and if you want, type a description.
4. If you want, click the Destination Log list and select the log in which you want to store the forwarded events. By default, events are stored in the Forwarded Events log.
5. Select the subscription type, which is either Collector Initiated or Source Computer Initiated. Selecting Collector Initiated causes the collecting computer to contact the forwarding computers, whereas selecting Source Computer Initiated causes the forwarding computers to contact the collecting computer. Then, specify the computers to use as follows:
   - If you selected Collector Initiated, click Select Computers. Click Add Domain Computers. In the Select Computer dialog box, type the name of the computer that will be forwarding events, and then click OK. In the Computers dialog box, click Test. Click OK when Event Viewer verifies connectivity.
   - If you selected Source Computer Initiated, click Select Computer Groups. Click Add Domain Computers or Add Non-Domain Computers. Type the name of the computer that will be forwarding events and click OK. If you added a non-domain computer, click Add Certificates and select a certification authority (CA) to be used to authenticate the source computers. Click OK.
6. Click Select Events and create the query filter. You must specify either a log or a source. Click OK.
7. If you want, click Advanced to open the Advanced Subscription Settings dialog box. You can configure three types of subscriptions:
   - **Normal** This option ensures reliable delivery of events and does not attempt to conserve bandwidth. It is the appropriate choice unless you need tighter control over bandwidth usage or need forwarded events delivered as quickly as possible. It uses *pull delivery mode* (where the collecting computer contacts the forwarding computer) and downloads five events at a time unless 15 minutes pass, in which case it downloads any events that are available.

- **Minimize Bandwidth** This option reduces the network bandwidth consumed by event delivery and is a good choice if you are using event forwarding across a wide area network or on a large number of computers on a local area network. It uses *push delivery mode* (where the forwarding computer contacts the collecting computer) to forward events every six hours.
- **Minimize Latency** This option ensures that events are delivered with minimal delay. It is an appropriate choice if you are collecting alerts or critical events. It uses push delivery mode and sets a batch timeout of 30 seconds.

  In addition, you can use this dialog box to specify whether the subscription uses HTTP or HTTPS as the protocol. If you create a collector-initiated subscription, you can use this dialog box to configure the user account that the subscription uses. Whether you use the default Machine Account setting or you specify a user, you need to ensure that the account is a member of the forwarding computer's Event Log Readers group.

8. Click OK to close the Advanced Subscription Settings dialog box.
9. In the Subscription Properties dialog box, click OK.

By default, normal event subscriptions check for new events every 15 minutes. You can decrease this interval to reduce the delay in retrieving events. However, there is no graphical interface for configuring the delay; you must use the command-line Windows Event Collector (Wecutil) tool that you initially used to configure the collecting computer.

To adjust the event subscription delay, first create your subscription using Event Viewer. Then, run the following two commands at an elevated command prompt:

wecutil ss <subscription_name> */cm:custom*

wecutil ss <subscription_name> */hi:*<milliseconds_delay>

For example, if you created a subscription named Critical Events and you wanted the delay to be 1 minute, you would run the following commands:

wecutil ss "Critical Events" /cm:custom

wecutil ss "Critical Events" /hi:6000

Now, if you open the Subscription Properties dialog box and click Advanced, the Advanced Subscription Settings dialog box shows the Event Delivery Optimization setting as Custom, as shown in Figure 8-3. This option is not selectable using the graphical interface.

If you need to check the interval, run the following command:

wecutil gs <subscription_name>

For example, to verify that the interval for the Critical Events subscription is 1 minute, you run the following command and look for the HeartbeatInterval value:

wecutil gs "Critical Events"

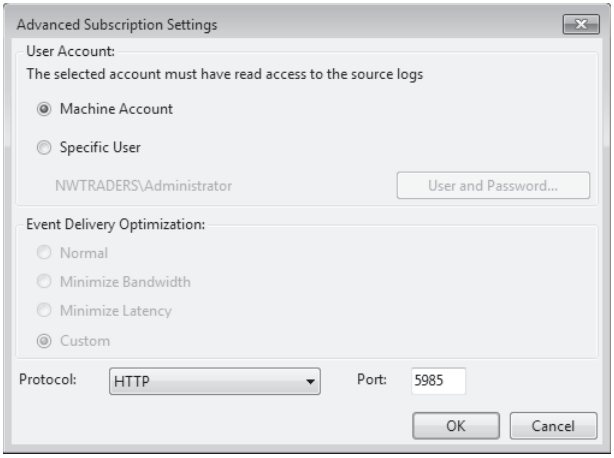

FIGURE 8-3 Configuring a custom Event Delivery Optimization with the Wecutil command-line tool

The Minimize Bandwidth and Minimize Latency options both batch a default number of items at a time. You can determine the value of this default by typing the following command at a command prompt:

winrm get winrm/config

How to Configure Event Forwarding to Use HTTPS

To configure event forwarding to use the encrypted HTTPS protocol, you must perform the following additional tasks on the forwarding computer in addition to those described in the section entitled "How to Configure the Forwarding Computer," earlier in this chapter:

1. Configure the computer with a computer certificate. You can do this automatically in AD DS environments by using an enterprise CA.
2. Create a Windows Firewall exception for TCP port 443.
3. Run the following command at an elevated command prompt: *winrm quickconfig –transport:https*

On the collecting computer, you must modify the subscription properties to use HTTPS rather than HTTP. In addition, the collecting computer must trust the CA that issued the computer certificate—this will happen automatically if the certificate was issued by an enterprise CA and both the forwarding computer and the collecting computer are part of the same AD DS domain.

If you have configured Minimize Bandwidth or Minimize Latency Event Delivery Optimization for the subscription, you must also configure a computer certificate and an HTTPS Windows Firewall exception on the collecting computer.

TIP **CHOOSING EVENTS TO FORWARD**

Windows 7 stores a great deal of very useful information in the event log, but there's even more useless information in there. For event forwarding, you should focus only on those events to which you can proactively respond.

To identify those useful events that you might want to forward, examine the event log each time a user calls with a problem. Did an event appear either shortly before or after the problem occurred? If so, and if the event appears only during problem scenarios, you should configure that event for forwarding.

How to Configure Event Forwarding in Workgroup Environments

Typically, event forwarding is required only in large environments that use AD DS domains. However, you can also configure event forwarding in workgroup environments. The process is very similar to that used in AD DS environments, with the following exceptions:

- You must add a Windows Firewall exception for Remote Event Log Management on each forwarding computer.
- You must add an account with administrator privileges to the Event Log Readers local group on each forwarding computer. You must specify this account in the Configure Advanced Subscription Settings dialog box when creating a subscription on the collector computer.
- On each collecting computer, run the following command to allow the forwarding computers to use NTLM authentication: *winrm set winrm/config/client @{TrustedHosts="*<forwarding_computers>*"}*.

  Provide a comma-separated list of forwarding computers for the *<forwarding computers>* value in the previous example. Alternatively, you can provide a wildcard, such as msft*.

EXAM TIP

For the exam, remember that you must configure the *TrustedHosts* parameter on the collecting computer, not the forwarding computer. This is counterintuitive and might be hard to remember.

Quick Check

1. **What command would you run to enable a collecting computer to use source computer–initiated subscriptions?**
2. **What protocols can event forwarding use?**
3. **Which group on the forwarding computer must the collecting computer be a member of?**

Quick Check Answers

1. You would run *winrm quickconfig*.
2. HTTP and HTTPS.
3. The Event Log Readers group.

How to Troubleshoot Event Forwarding

If event forwarding doesn't seem to function properly, follow these steps to troubleshoot the problem:

1. Verify that you have waited long enough for the event to be forwarded. Forwarding events using the Normal setting can take up to 15 minutes. The delay might be longer if either the forwarding or the collection computer has restarted recently because the Windows Remote Management service is set to start automatically, but with a delay so that it doesn't affect startup performance. The 15-minute counter doesn't start until after the Windows Remote Management service has started.
2. Check the Applications And Services Logs\Microsoft\Windows\Eventlog-ForwardPlugin\Operational event log and verify that the subscription was created successfully. Event ID 100 indicates a new subscription, whereas Event ID 103 indicates a subscription has been unsubscribed.
3. Check the Security event log to verify that the forwarding and collecting computers are authenticating correctly. If necessary, enable success and failure auditing as described in Chapter 4, "Security."
4. Verify that the subscription is Active. On the collecting computer, browse to Event Viewer\Subscriptions. The subscription status should be Active. If it is not, right-click the subscription and then click Runtime Status. Event Viewer displays the Subscription Runtime Status dialog box with an error code.
5. Verify that the forwarding computer has the Windows Remote Management listener properly configured. From an elevated command prompt, run the following command: *winrm enumerate winrm/config/Listener*.

   If the Windows Remote Management listener isn't configured, there is no output. If the Windows Remote Management listener is configured properly for HTTP, the output resembles the following:

```
Listener
   Address = *
   Transport = HTTP
   Port = 80
   Hostname
   Enabled = true
   URLPrefix = wsman
   CertificateThumbprint
   ListeningOn = 127.0.0.1, 192.168.1.214, ::1, fe80::100:7f:ffe%9,
                 fe80::5efe:192.168.1.214%10
```

If the Windows Remote Management listener is configured properly for HTTPS, the output resembles the following (note that the host name must match the name the event collector uses to identify the computer):

```
Listener
   Address = *
   Transport = HTTPS
   Port = 443
   Hostname = win7.nwtraders.msft
   Enabled = true
   URLPrefix = wsman
   CertificateThumbprint = 52 31 db a8 45 50 1f 29 d9 3e 16 f0 da 82 ae
                           94 18 8f 61 5e
   ListeningOn = 127.0.0.1, 192.168.1.214, ::1, fe80::100:7f:ffe%9,
                 fe80::5efe:192.168.1.214%10
```

6. Verify that the collecting computer can connect to Windows Remote Management on the forwarding computer. From an elevated command prompt on the collecting computer, run the following command: *winrm id –remote:<computer_name>.<domain_name>*.

   For example, if the forwarding computer is named win7.nwtraders.msft, you would run the following command: *winrm id –remote:win7.nwtraders.msft*.

   The result would be as follows:

   ```
   IdentifyResponse
      ProtocolVersion = http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
      ProductVender = Microsoft Corporation
      ProductVersion = OS: 6.0.6000 SP: 0.0 Stack: 1.0
   ```

   If you receive the message "WS-Management could not connect to the specified destination," verify that the Windows Remote Management service is started on the forwarding computer and that no firewall is blocking connections between the two computers.

7. Verify that the user account you configured the subscription to use has privileges on the forwarding computer. If necessary, enable failure security auditing on the remote computer as described in Chapter 4, wait for events to be forwarded, and then examine the Security event log for logon failures. In addition, you can configure the subscription temporarily to use a Domain Admin account—if the subscription works with the Domain Admin account, the source of your problem is definitely related to authentication. Troubleshoot the authentication problem and reconfigure the subscription to use the original user account.

8. If the subscription is configured to use Machine Account authentication, verify that the collecting computer's account is a member of the forwarding computer's Event Log Readers local group. If the subscription is configured to use a different user account, that account must be in the forwarding computer's Event Log Readers local group.

9. Verify that the following services are started on the forwarding computer:
   - Windows Remote Management (WS-Management)
   - Windows Event Collector
10. Verify that the Windows Event Collector service is started on the collecting computer.
11. Verify Windows Firewall settings on the forwarding computer as follows:
   - Verify that the Windows Remote Management (HTTP-In) firewall exception is enabled.
   - If you are using HTTPS instead of HTTP, verify that you have created and enabled a custom firewall exception for TCP port 443.
   - Verify that the forwarding computer and the collecting computer are both connected to Private or Domain networks, rather than to Public networks. To verify the network profile, right-click the network icon in the system tray and then click Open Network And Sharing Center. In the Network And Sharing Center, the profile type appears after the network name. If it shows Public Network, click Customize and change the profile type to Work Network, which uses the private network profile.
12. In addition to the forwarding computer, verify that the Windows Remote Management (HTTP-In) firewall exception is enabled on the collecting computer.
13. Verify that a network firewall is not blocking traffic by testing connectivity. Because the forwarding computer must have HTTP (and possibly HTTPS) available, you can attempt to connect to it from the collecting computer by using Windows Internet Explorer—simply type **http://*computername*** (or **https://*computername*** if you are using HTTPS) in the Address bar. If the firewall on the forwarding computer is configured correctly, you receive an HTTP 404 error and Internet Explorer displays the message, "The webpage cannot be found." If Internet Explorer displays the message, "Internet Explorer cannot display the webpage," the firewall exception on the forwarding computer has not been enabled.
14. Verify that the event query is valid by performing these steps:
   a. View the subscription properties, and click Select Events.
   b. Select the XML tab, select the contents of the query, and press Ctrl+C to copy it to the Clipboard.
   c. Open a second instance of Event Viewer. Right-click Event Viewer, and then click Connect To Another Computer. Select the forwarding computer, and then click OK.
   d. Right-click Custom Views, and then click Create Custom View.
   e. In the Create Custom View dialog box, select the XML tab. Select the Edit Query Manually check box, and click Yes when prompted.
   f. Click the query box and press Ctrl+V to paste the query. Then click OK.
   g. The new custom view appears and shows the matching events. If any events have appeared since you created the event forwarder, they should have been forwarded. If there are no new events, the problem is with your forwarding criteria. Try creating a custom view that matches the events that you want to forward and then importing that into a new subscription.

PRACTICE Forward Events Between Computers

In this practice, you configure event forwarding between two computers using the default settings.

EXERCISE 1 Configuring a Computer to Collect Events

In this exercise, you configure a computer to collect events.

1. Log on to the computer running Windows 7 that you want to use to collect events using a domain account with administrative privileges.
2. Open an elevated command prompt by clicking Start, typing **cmd**, and pressing Ctrl+Shift+Enter.
3. At the command prompt, run the following command to configure the Windows Event Collector service:

   ```
   wecutil qc
   ```

4. When prompted to change the service startup mode to Delay-Start, type **Y**, and then press Enter.

EXERCISE 2 Configuring a Computer to Forward Events

In this exercise, you configure a computer running Windows 7 to forward events to the collecting computer. To complete this exercise, you must have completed Exercise 1.

1. Log on to the computer running Windows 7 that you want to use to forward events using a domain account with administrative privileges.
2. Open an elevated command prompt by clicking Start, typing **cmd**, and pressing Ctrl+Shift+Enter.
3. At the command prompt, run the following command to configure the Windows Remote Management service: *winrm quickconfig*.
4. When prompted to change the service startup mode, type **Y**, and then press Enter.
5. When prompted to create the WinRM listener and enable the firewall exception, type **Y** and then press Enter.
6. Verify that you have updated the Windows Firewall configuration by following these steps:
   a. Click Start and then click Control Panel.
   b. Click the System And Security link.
   c. Click the Windows Firewall link.
   d. Click the Advanced Settings link.
   e. Select the Inbound Rules node.
   f. In the Details pane, verify that the Windows Remote Management (HTTP-In) exception is enabled for the Domain and Private profiles.

7. Verify that the Windows Remote Management service is configured to start automatically by following these steps:
   a. Click Start, type **services.msc**, and then press Enter.
   b. In the Services console, select the Windows Remote Management (WS-Management) service. Verify that it is started and that the Startup Type is set to Automatic (Delayed Start).
8. Now you need to grant the collecting computer permission to read this computer's event log. If you skipped this step, you would need to configure the subscription to use an administrative user account. To grant access to the collecting computer account, perform these steps:
   a. Click Start, right-click Computer, and then click Manage.
   b. Under System Tools, expand Local Users And Groups. Then, select Groups.
   c. Double-click Event Log Readers.
   d. In the Event Log Readers Properties dialog box, click Add.
   e. In the Select Users, Computers, Service Accounts, Or Groups dialog box, click Object Types. By default, it searches only Users and Groups. However, we need to add the collecting computer account. Select the Computers check box and clear the Groups, Users, and Service Accounts check boxes. Click OK.
   f. In the Select Users, Computers, Or Groups dialog box, type the name of the collecting computer. Then, click OK.
   g. Click OK again to close the Event Log Readers Properties dialog box.

EXERCISE 3 Configuring an Event Subscription

In this exercise, you create an event subscription to gather events from the forwarding computer. To complete this exercise, you must have completed Exercises 1 and 2.

1. Log on to the computer running Windows 7 that you want to use to collect events using a domain account with administrative privileges.
2. Click Start, right-click Computer, and then click Manage.
3. In the Computer Management console, expand System Tools, expand Event Viewer, right-click Subscriptions, and then click Create Subscription.
4. In the Event Viewer dialog box, click Yes to configure the Windows Event Collector service (if prompted).

   The Subscription Properties dialog box appears.
5. In the Subscription Name box, type **Windows Defender Warnings And Errors**.
6. Click Select Computers. In the Computers dialog box, click Add Domain Computers. Type the name of the computer that will be forwarding events, and then click OK. In the Computers dialog box, click Test to verify that you can connect to the forwarding computer. Click OK twice.

7. Click Select Events. In the Query Filter dialog box, select the Error, Critical, Warning, and Information check boxes. Click By Source. Then, click the Event Sources list and select Windows Defender (as shown in Figure 8-4). Click OK.

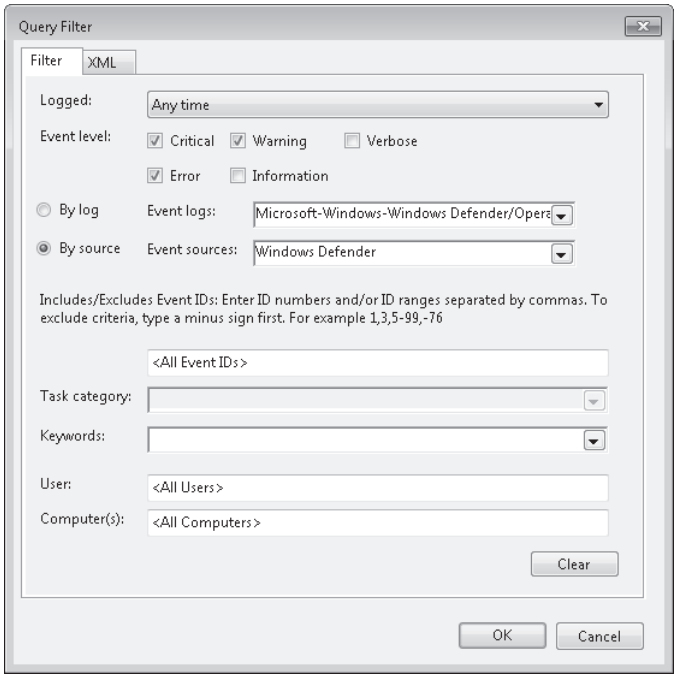

FIGURE 8-4 Configuring the Query Filter to forward important Windows Defender events

8. Click Advanced to open the Advanced Subscription Settings dialog box. Note that it is configured to use the Machine Account by default. This works because we have added this computer's domain account to the forwarding computer's Event Log Readers local group. Also, note that the subscription is configured by default to use Normal Event Delivery Optimization using the HTTP protocol. Click OK.
9. In the Subscription Properties dialog box, click OK.
10. Next, generate a Windows Defender event on the forwarding computer by following these steps:
    a. Log on to the forwarding computer.
    b. Click Start and type **Defender**. On the Start menu, click Scan For Spyware And Other Potentially Unwanted Software.

    Windows Defender scans the computer and adds an event to the event log.
11. While still using the forwarding computer, open Event Viewer and check the Applications And Services Logs\Microsoft\Windows\Windows Defender\Operational log. You should see several Informational events with a source of Windows Defender.

12. Using the collecting computer, select the Forwarded Events event log. If you don't see the Windows Defender event immediately, wait a few minutes—it might take up to 15 minutes for the event to appear.

Lesson Summary

- Event forwarding uses HTTP by default, allowing it to pass easily through most firewalls. You can also configure event forwarding to use HTTPS. However, communications are encrypted with standard HTTP.
- To configure event forwarding in a domain, run the *winrm quickconfig* command at the forwarding computer and run the *wecutil qc* command on the collecting computer. Then, add the collecting computer's account to the forwarding computer's Event Log Readers group.
- To configure event forwarding in a workgroup, follow the same steps that you would in a domain. In addition, you need to add a Windows Firewall exception for the Remote Event Log Management service on each forwarding computer, add a user account with administrator privileges to the forwarding computer's Event Log Readers group, and run the *winrm set* command to configure the collecting computer to trust the forwarding computers.
- To troubleshoot event forwarding, verify that you have waited long enough and that subscriptions are active, check the Windows Remote Management configuration on both the forwarding and collecting computers, and verify that the user account you specified for the subscription is a member of the forwarding computer's Event Log Readers group.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Forwarding Events." The questions are also available on the companion CD if you prefer to review them in electronic form.

> ***NOTE*** **ANSWERS**
>
> **Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.**

1. When starting with the default configuration of a computer, which of the following steps are required to enable event forwarding? (Choose all that apply.)
   - **A.** Start the Windows Remote Management service on the forwarding computer.
   - **B.** Start the Windows Remote Management service on the collecting computer.
   - **C.** Configure Microsoft Internet Information Services (IIS) on the forwarding computer.
   - **D.** Enable a Windows Firewall exception on the forwarding computer.
   - **E.** Nothing is required; event forwarding is enabled by default.

2. Which tool would you use to configure a subscription to use a 10-minute interval?
   - **A.** Event Viewer
   - **B.** Winrm
   - **C.** Wecutil
   - **D.** Wevutil
3. What is the standard interval for a subscription with a bandwidth optimization setting of Minimize Latency?
   - **A.** 30 seconds
   - **B.** 15 minutes
   - **C.** 30 minutes
   - **D.** 6 hours
4. Which of the following tasks do you need to perform in an AD DS domain environment to enable a computer to collect events from another computer?
   - **A.** Run the following command on the collecting computer: *winrm set winrm/config/client @{TrustedHosts="*<forwarding_computers>*"}*.
   - **B.** Run the following command on the forwarding computer: *winrm set winrm/config/client @{TrustedHosts="*<collecting_computers>*"}*.
   - **C.** Add the forwarding computer's machine account to the Event Log Readers local group.
   - **D.** Add the collecting computer's machine account to the Event Log Readers local group.

Lesson 2: Troubleshooting Performance Problems

When a user experiences a performance problem, you need to know how to identify the source of the problem quickly and, if necessary, resolve it. Fortunately, Windows 7 provides Task Manager to give you an overview of system performance. Task Manager also allows you to change the priority and affinity of a process to limit the processing resources it can consume. With Performance Monitor, you can examine thousands of details about system and application performance in real time, or log the data for later analysis.

Data collector sets create a snapshot of a system's state, storing detailed information about a computer's configuration for later analysis. If you identify disk input/output time as the source of a performance problem, you might be able to resolve it by freeing up disk space and defragmenting the disk. For mobile computers, you must consider settings that compromise system performance in favor of extended battery life. If a problem seems to be related to a startup service or application, you can use the System Configuration tool to selectively disable startup processes until you identify the process causing the problem.

After this lesson, you will be able to:

- Use Task Manager to examine system performance and control individual processes.
- Use Performance Monitor to examine real-time statistics and compare logged data to a performance baseline.
- Use data collector sets to generate reports that provide detailed information about a computer's configuration and the problems it's experiencing.
- Troubleshoot disk performance problems by freeing wasted disk space.
- Adjust how mobile computers optimize performance and battery life to meet users' needs.
- Use the System Configuration tool to disable startup services and applications selectively.

Estimated lesson time: 45 minutes

Task Manager

Task Manager is the quickest way to identify common performance problems. Windows 7 makes it easy to open Task Manager even if the user interface isn't responding correctly. You can open Task Manager in the following ways:

- Right-click the taskbar or the system clock and then click Start Task Manager.
- Press Ctrl+Alt+Del, and then click Start Task Manager. You can do this even if the user interface is completely non-responsive.

Task Manager has six tabs:

- **Applications** A list of applications open by the current user. You can close an application by clicking it and then clicking End Task. If the Start menu is not working, you can start a new application by clicking New Task. If the Windows Explorer interface is not open, you can click New Task and then run Windows Explorer to open it.
- **Processes** A list of processes open by the current user. You can view processes open by all users by clicking Show Processes From All Users. You can quickly identify the process that is using the most processor time by clicking the CPU column header to sort the processes by processor utilization. To end a process, select the process and then click End Process. Ending a process is particularly useful when a non-responsive application is consuming all the processor time and slowing the computer down.
- **Services** Lists all the services on the computer, running or stopped. You can start and stop services by right-clicking the service. This tab provides similar functionality to the Services console, but with the convenience of Task Manager.
- **Performance** Shows current processor and memory utilization. If a computer seems slow, open the Performance tab to determine whether processor or memory utilization is causing the problem. If processor utilization is causing the problem, one or more of the processors in the CPU Usage History chart will be at 100%, as the first processor is in Figure 8-5. If memory utilization is causing the problem, the value shown in the Memory chart will be close to the Total value shown in the Physical Memory group.

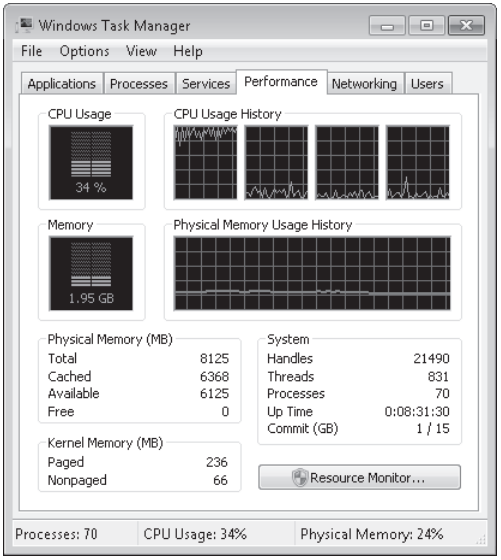

FIGURE 8-5 Task Manager shows processor and memory utilization.

- **Networking** Charts the network utilization of each network interface. Use this tab to determine whether a slow network might be caused by an application using all the available bandwidth. Wired network connections typically do not support more than 70% utilization; therefore, a wired network at 65% utilization can be considered

completely saturated. Available bandwidth for wireless network connections varies, but is typically around 35% as shown by the charts on the Networking tab.

- **Users** Lists the users currently logged on to the computer.

The sections that follow discuss how to perform different tasks with Task Manager.

How Windows Shares Processor Time Between Applications

To understand how to troubleshoot performance, you must know how applications, processes, and threads relate. An application or service typically has a single process associated with it, though some applications or services might start multiple processes. Processes run within threads. Every application has at least one thread, and it might start multiple threads. Some applications might use hundreds of threads.

A processor (or processor core) can only run one thread at a time. A computer with one processor can still run multiple applications, however, because Windows switches the processor between different processes and threads. Higher-priority threads receive more processor time than lower-priority threads.

Today, most new computers have processors with multiple cores. Each processor core functions like a separate processor. If you view the Performance tab of Task Manager, the CPU Usage graph shows the total utilization across all processors, and the CPU Usage History graph shows a separate graph for each processor core. If you see only one graph in the CPU Usage History box, click the View menu, click CPU History, and then click One Graph Per CPU.

One of the most important tasks Windows performs is distributing processor time. With multiple applications running, many having multiple threads, and multiple processor cores, the task of distributing processor time can be very complicated. Fortunately, as Figure 8-6 illustrates, Windows handles it automatically, and you rarely need to adjust the default settings.

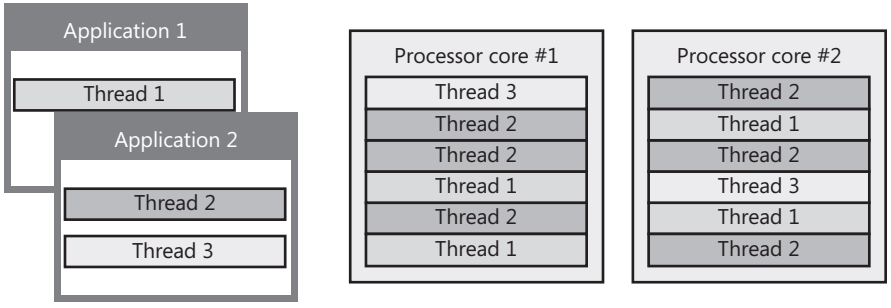

FIGURE 8-6 Windows assigns threads processor time.

There are some circumstances that might require you to control processes manually:

- A single process is using too much processor time, slowing down other processes.
- Applications are utilizing the processor fully, and you want one application to receive more or less processor time than other applications.
- An application is not responding, and you want to end the application's processes forcibly.

The sections that follow show you how to accomplish each of these.

How to Identify Which Program Is Using the Most Processor Time

You can use Task Manager to identify a process that is using excessive processor time. Optionally, you can end the process forcibly by performing these steps:

1. Start Task Manager.
2. On the Processes tab, click the CPU column heading.
3. The process consuming the most processor time is shown at the top of the list.
4. With the busiest process identified, you can change the priority of the process (which might improve the performance of other applications), end the process, or limit the process to specific processor cores by performing either of the following:
   - To change the priority of the process, right-click the process, select Set Priority, and then click the desired priority. Lower-priority processes receive less processor time, whereas higher-priority processes receive more processor time. Most processes run with Normal priority. Task Manager is a notable exception; it runs at High priority by default so that you can use it if another application is consuming significant amounts of processor time. Avoid giving any process Realtime priority, because it might slow the user interface.
   - By default, Windows can assign a process to run on any processor core. To limit the process to specific processor cores on a computer with multiple cores, right-click the process and then click Set Affinity. Figure 8-7 shows the Processor Affinity dialog box, which allows you to select which processor cores a process can use. Figure 8-7 shows Iexplore.exe (the Internet Explorer process) limited to two out of four processor cores, ensuring Internet Explorer never uses more than half the total processor time. Closing and restarting a process resets the processor affinity.

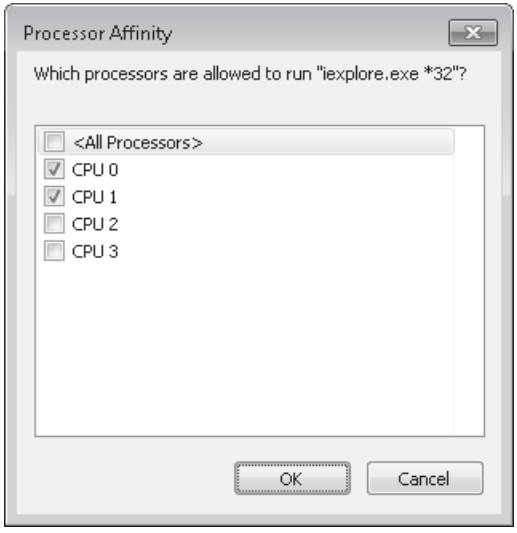

FIGURE 8-7 The Processor Affinity dialog box allows you to limit the processor cores on which a process can run.

- To end the process, right-click the process and then click End Process. Alternatively, you can click End Process Tree to end any processes that process started.

How to Stop a Program

Occasionally, a program might not respond. Typically, you can right-click the application on the task bar and then click Close Window. In a few seconds, Windows prompts you to terminate the nonresponsive application.

If that approach does not work, you can use Task Manager to close an application as follows:

1. In Task Manager, on the Applications tab, select the application.
2. Click End Task.
3. If Task Manager cannot end the application, the End Program dialog box appears. Click End Now.

If you want to identify which process is associated with an application, right-click the application on the Applications tab, and then click Go To Process.

Performance Monitor

Like earlier versions of Windows, the Performance Monitor snap-in graphically displays real-time data, as shown in Figure 8-8.

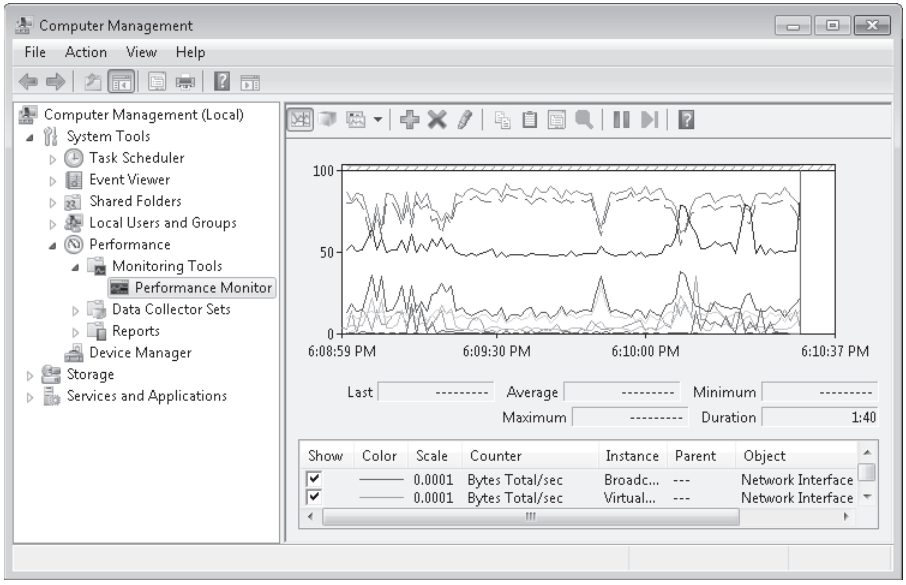

FIGURE 8-8 How Performance Monitor shows real-time data

The sections that follow describe how to monitor real-time data, how to configure the Performance Monitor chart, and how to compare multiple graphs.

How to Monitor Real-Time Performance Data

To open Performance Monitor, follow these steps:

1. Click Start, right-click Computer, and then click Manage.
2. Expand System Tools, expand Performance, and then expand Monitoring Tools. Select Performance Monitor.
3. Add counters to the real-time graph by clicking the green plus button on the toolbar. You can also display data from other computers on the network.

Each line on the graph appears in a different color. To make it easier to view a specific graph, select a counter and press Ctrl+H. The selected counter appears bold and in black on the graph.

Performance Monitor automatically assigns line colors and styles to the counters you select. To configure line colors and styles manually, follow these steps:

1. Click the Action menu, and then click Properties.

   The Performance Monitor Properties dialog box appears.
2. Click the Data tab.
3. In the Counters list, select the counter you want to configure. Then, adjust the Color, Width, and Style settings.
4. To increase the height of the graph for a counter, click the Scale list and click a higher number. To decrease the height of a graph, click the Scale list and click a lower number.
5. You can also adjust the scale for all counters by clicking the Graph tab and changing the Maximum and Minimum values in the Vertical Scale group. Click OK.

If you keep multiple Performance Monitor windows open simultaneously, you can make it easier to quickly distinguish between the windows by changing the background color on the chart using the Appearance tab in the Performance Monitor Properties dialog box.

How to Control How Much Data Appears in the Graph

By default, Performance Monitor updates the graphs once per second and displays 100 seconds of data. To display data over a longer period of time, you can increase the sampling interval or increase the amount of data displayed on the graph at once. To adjust these settings, follow these steps in Performance Monitor:

1. Click the Action menu, and then click Properties.

   The Performance Monitor Properties dialog box appears.
2. In the General tab, in the Graph Elements group, adjust the Sample Every box to change how frequently the graph updates. Use a longer interval (such as five seconds) to show a smoother, less jagged graph that is updated less frequently. If you are connecting to a computer across a network, longer intervals reduce bandwidth usage.

3. Adjust the Duration box to change how much data is displayed in the graph before Performance Monitor begins overwriting the graph on the left portion of the chart. To display one full hour of data in the graph, set the duration to 3,600. To display one full day of data in the graph, set the duration to 86,400. If you increase the Duration box, you should also increase the Sample Every box. Click OK.

By default, Performance Monitor begins overwriting graphed data on the left portion of the chart after the specified duration has been reached. When graphing data over a long period of time, it's typically easier to see the chart scroll from right to left, similar to the way Task Manager shows data. To configure the Performance Monitor graph to scroll data, perform these steps:

1. Click the Action menu, and then click Properties.

   The Performance Monitor Properties dialog box appears.

2. Click the Graph tab. In the Scroll Style group, select Scroll. Click OK.

Although the line chart shows the most information, you can select from the following chart types by clicking the Change Graph Type button on the toolbar or by pressing Ctrl+G:

- **Line** The default setting, this shows values over time as lines on the chart.
- **Histogram bar** This shows a bar graph with the most recent values for each counter displayed. If you have a large number of values and you're primarily interested in the current value (rather than the value of each counter over time), this will be easier to read than the line chart.
- **Report** This text report lists each current value.

Data Collector Sets and Reports

Previous versions of Windows enabled you to log performance counter data and view it later. Windows Vista and Windows 7 greatly expand this capability. Now you can create a data collector set to log the following types of information:

- Performance counters and alerts (just like in previous versions of Windows)
- Event trace data showing detailed debugging information
- Registry settings showing system and application configuration

After running a data collector set, you can view the performance counters in Performance Monitor and you can view a summary of the other collected information in a report. The sections that follow describe how to create data collector sets and how to use reports.

Built-in Data Collector Sets

Windows 7 includes several built-in data collector sets located at Performance\Data Collector Sets\System:

- **System Performance** Logs processor, disk, memory, and network performance counters and kernel tracing. Use this data collector set when troubleshooting a slow computer or intermittent performance problems.
- **System Diagnostics** Logs all the information included in the System Performance data collector set, plus detailed system information. Use this data collector set when troubleshooting reliability problems such as problematic hardware, driver failures, or Stop errors. As shown in Figure 8-9, the report generated by the data collector set provides a summary of error conditions on the system without requiring you to browse Event Viewer and Device Manager manually.

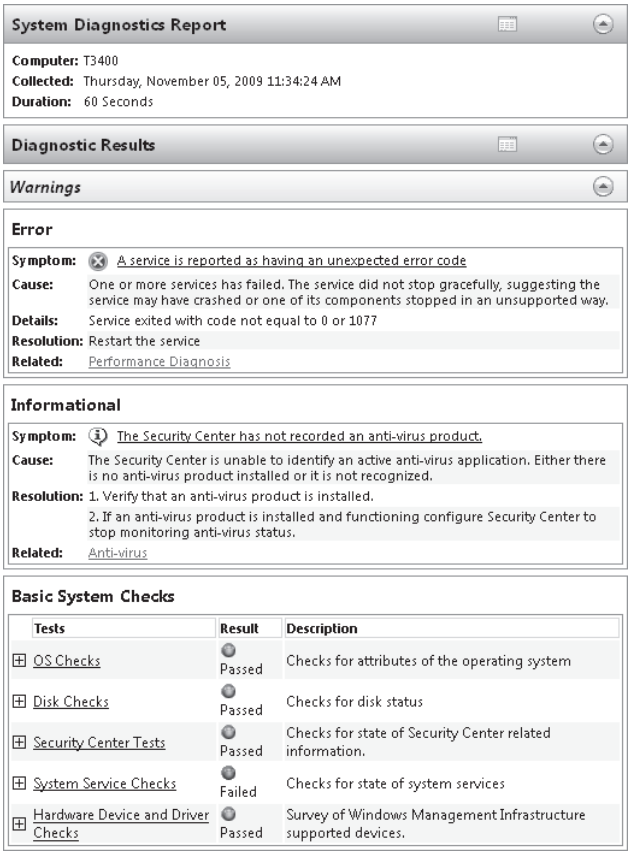

FIGURE 8-9 The System Diagnostics Report

To use a data collector set, right-click it, and then click Start. The System Performance data collector set stops automatically after a minute, and the System Diagnostics data collector set stops automatically after 10 minutes. To stop a data collector set manually, right-click it, and then click Stop.

After running a data collector set, you can view a summary of the data gathered in the Performance\Reports node. To view the most recent report for a data collector set, right-click the data collector set, and then click Latest Report. Reports are named automatically using the format *<Computer_Name>_yyyymmdd-######*.

To minimize the performance impact of data logging, log the least amount of information required. For example, you should use System Performance instead of System Diagnostics whenever possible because System Performance includes fewer counters.

When a problem is difficult to reproduce and is not performance-related, you should err on the side of logging too much data to minimize the chance that you will miss important information.

How to Create a Data Collector Set Using a Standard Template

You can save performance data to a log and then view and analyze the data in Performance Monitor at any time. It's important to create a *baseline* by logging performance data before making changes that you think might have a performance impact. After making the changes, you can compare new performance data to the original performance data to determine whether your changes were beneficial. If you don't have a baseline available when a problem appears, you can create one using a different computer with a similar configuration that does not have the problem.

To save performance data, follow these steps:

1. Under Performance, expand Data Collector Sets.
2. Right-click User Defined, click New, and then click Data Collector Set.

   The Create New Data Collector Set Wizard appears.
3. On the How Would You Like To Create This New Data Collector Set? page, type a name for the set. Make sure Create From A Template is selected. Then, click Next.
4. On the Which Template Would You Like To Use? page, choose from one of the three standard templates (or Browse to select a custom template) and click Next:
   - **Basic** Logs all Processor performance counters, stores a copy of the HKLM\Software\Microsoft\Windows NT\CurrentVersion registry key, and performs a Windows Kernel Trace.
   - **System Diagnostics** Logs 13 useful performance counters (including processor, disk, memory, and network counters), stores a copy of dozens of important configuration settings, and performs a Windows Kernel Trace. By default, System Diagnostics logs data for one minute, giving you a snapshot of the computer's status.
   - **System Performance** Logs 14 useful performance counters (including the same counters logged by the System Diagnostics template) and performs a Windows Kernel Trace. System Performance logs data for one minute.
5. On the Where Would You Like The Data To Be Saved? page, click Next to accept the default location for the data (%Systemdrive%\Perflogs\Admin).

6. On the Create The Data Collector Set page, leave Run As set to <Default> to run it using the current user's credentials, or click Change to specify other administrative credentials. Select one of three options before clicking Finish:
   - **Open Properties For This Data Collector Set** Immediately customize the Data Collector Set.
   - **Start This Data Collector Set Now** Immediately begin logging data without customizing the Data Collector Set.
   - **Save And Close** Close the Data Collector Set without starting it. You can edit the properties and start it at any time after saving it.

Custom data collector sets are always available under the User Defined node within Data Collector Sets.

How to Create a Custom Data Collector Set

After creating a new data collector set, you can modify it to log additional data sources by right-clicking the data collector set, clicking New, and then clicking Data Collector to open the Create New Data Collector wizard. On the What Type Of Data Collector Would You Like To Create? page, type a name for the data collector, select the type, and then click Next.

You can choose from the following types of data collectors (each of which provides different options in the Create New Data Collector wizard):

- **Performance Counter Data Collector** Logs data for any performance counter available when using the Performance Monitor console. You can add as many counters as you like to a data collector. You can assign a sample interval (15 seconds, by default) to the data collector.
- **Event Trace Data Collector** Stores events from an event trace provider that match a particular filter. Windows 7 provides dozens of event trace providers that are capable of logging even the most minute aspects of the computer's behavior. For best results, simply add all event trace providers that might relate to the problem you are troubleshooting. If the data collector logs a large amount of unnecessary data, you can use the provider properties to filter which trace events are stored.
- **Configuration Data Collector** Stores a copy of specific registry keys, management paths, files, or the system state. If you are troubleshooting application problems or if you need to be aware of application settings, add the registry keys using a configuration data collector. To add a management path, file, or system state, create the data collector without specifying a registry key using the wizard. Then, view the new data collector properties, and select the Management Paths, File Capture, or State Capture tab.
- **Performance Counter Alert** Generates an alert when a performance counter is above or below a specified threshold.

You can add as many data collectors to a data collector set as required.

How to Save Performance Data

After creating a data collector set, you can gather the data specified in the Data Collector Set by right-clicking it and clicking Start. Depending on the settings configured in the Stop Condition tab of the data collector set's Properties dialog box, the logging might stop after a set amount of time or it might continue indefinitely. If it does not stop automatically, you can manually stop it by right-clicking it and clicking Stop.

How to View Saved Performance Data in a Report

After using a data collector set to gather information and then stopping the data collector set, you can view the gathered information. To view a summary of the data saved using a data collector set, right-click the data collector set and then click Latest Report. The console expands the Reports node and selects the report generated when the data collector set ran. You can expand each section to find more detailed information.

If the data collector set included performance counters, you can also view them using the Performance Monitor snap-in by following these steps:

1. Under Performance, expand Monitoring Tools, and then select Performance Monitor.
2. Click the Action menu, and then click Properties. In the Performance Monitor Properties dialog box, click the Source tab. You can also click the View Log Data button on the toolbar or press Ctrl+L.
3. Under Data Source, select Log Files. Then, click Add. By default, Windows 7 stores data collector set data in the C:\Perflogs\ folder. Browse to select the data collector set data (the folder corresponds to the report name), and then click Open.
4. If you want, click Time Range and narrow the range of data you want to analyze.
5. Click OK.
6. In Performance Monitor, click the green Add button on the toolbar and add counters to the chart. Because you specified a data source, you can add only counters that were logged.
7. Performance Monitor shows the logged data instead of real-time data. To narrow the time range shown, click and drag your cursor over the graph to select a time range. Then, right-click the graph and click Zoom To, as shown in Figure 8-10.
8. The horizontal bar beneath the graph illustrates the currently selected time range. Drag the left and right sides of the bar to expand the selected time range. Then, right-click the graph and click Zoom To again to change the selection.

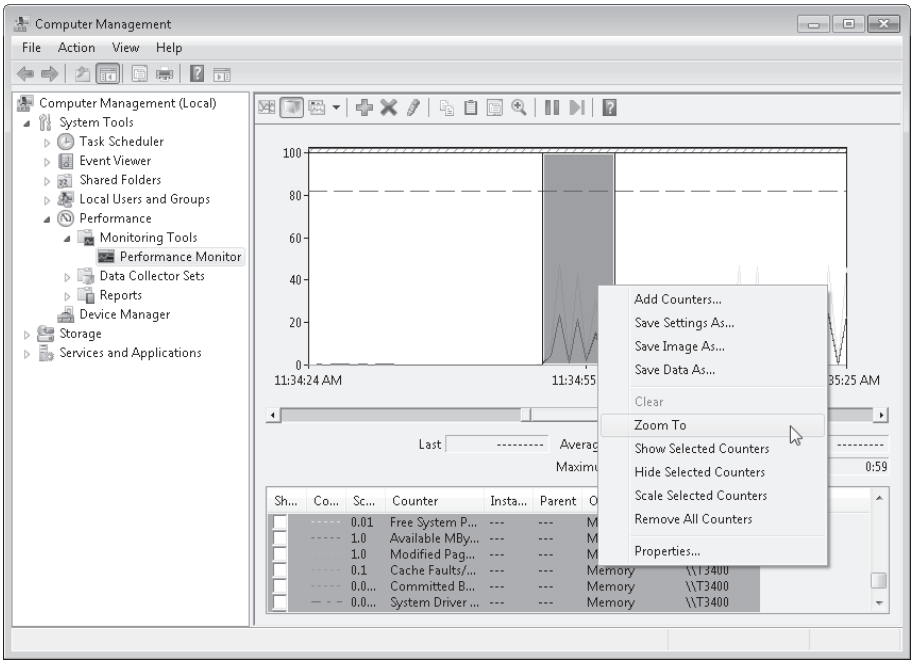

FIGURE 8-10 Using the Zoom To feature to analyze a narrow time span

Troubleshooting Disk Performance Problems

For many common tasks on a computer, the hard disk limits overall performance. Opening and saving files requires reading from and writing to the hard disk, which is much slower than accessing system RAM. In addition, if Windows needs to allocate more memory than it has physical RAM available, Windows uses the hard disk as virtual memory, reducing performance for any task that requires the memory stored on the hard disk.

Fortunately, there are several things you can do to improve performance without upgrading to a faster hard disk. The sections that follow discuss fragmentation and virtual memory.

Fragmentation and Free Space

To reduce fragmentation, increase the amount of free disk space. When a disk begins to run out of space, Windows needs to divide files into several different fragments, a process known as *fragmentation*. Because hard disks perform best when a file is not fragmented, fragmentation slows disk performance. As a general rule, you should keep at least 15 percent of a disk's space free, but having more free disk space can further improve performance.

NOTE **FRAGMENTATION AND FLASH DRIVES**

Traditional, magnetic hard disks have a drive head that must move across several spinning round platters to read data, much like a record player. These drives perform best when reading and writing sequentially, which does not require the drive head to move to a different part of the disk. To read a fragmented file, the drive head must move several times, slowing performance.

Flash drives do not have a drive head, and fragmentation does not reduce their performance. Therefore, you never have to worry about fragmentation with a flash drive. Windows 7 automatically disables defragmentation for flash drives.

You can use the Windows 7 Disk Cleanup tool to free up disk space automatically by following these steps:

1. Click Start, and then click Computer.
2. Right-click the drive you want to clean, and then click Properties.
3. On the General tab, click Disk Cleanup.
4. To remove system files (a task that requires administrative privileges), click Clean Up System Files.
5. Select the files that you want to delete. You can click each file type for a description of the files that will be removed. Click OK.

   The Disk Cleanup tool removes the files you specified.

Windows 7 automatically defragments your files, so you should never need to defragment manually. If you would like to defragment files manually, perform these steps:

1. Click Start, and then click Computer.
2. Right-click the drive you want to defragment, and then click Properties.
3. On the Tools tab, click Defragment Now.
4. To configure the defragmentation schedule, click Configure Schedule.
5. In the Disk Defragmenter tool, select the disk you want to defragment, and then click Defragment Disk.

   The Disk Defragmenter begins defragmenting the drive. You don't have to wait for it to complete before closing the window, however.
6. Click Close, and then click OK.

Virtual Memory

Depending on the disk configuration, you can maximize the performance of virtual memory by storing virtual memory on a different physical hard disk from other files. For example, if a computer has a separate C: and D: drive, Windows by default uses the C: drive for virtual memory. By moving the virtual memory to the D: drive, Windows might be able to read and write files stored on the C: drive at the same time it accesses virtual memory.

NOTE **STORING VIRTUAL MEMORY ON A SEPARATE DISK**

Although you can achieve performance benefits by storing virtual memory on a separate hard disk, you will not see any benefits by storing virtual memory on a different volume or partition of a single hard disk. For best performance with multiple disks, configure the disks in a redundant array of independent disks (RAID) array, and store all data on that RAID array.

To configure which disk Windows stores virtual memory on, perform these steps:

1. Click Start, right-click Computer, and then click Properties.
2. Click Advanced System Settings.
3. On the Advanced tab of the System Properties dialog box, click Settings in the Performance group.
4. On the Advanced tab of the Performance Options dialog box, click Change.
5. Clear the Automatically Manage Paging File Size For All Drives check box.
6. Select the drive that you want to use to store virtual memory (also known as a *paging file*). Click System Managed Size, and then click OK.
7. Select the system drive which currently has the paging file assigned to it. Click No Paging File, and then click Set. Figure 8-11 shows a computer that has had virtual memory assigned to the G: drive and removed from the default C: drive. Click Yes when prompted.

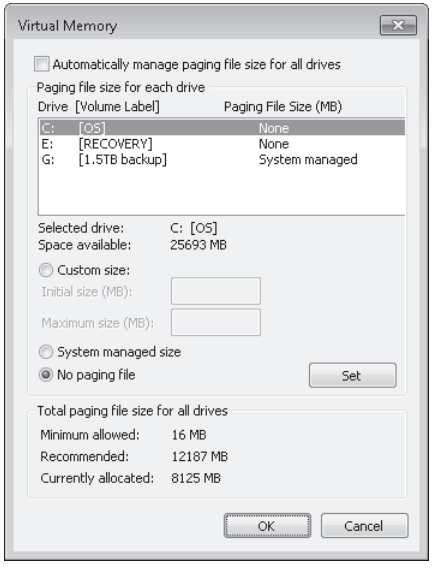

FIGURE 8-11 Configuring virtual memory storage

8. Click OK four times, and then click Restart Now to restart your computer.

Configuring Power Settings

Some aspects of a computer are a compromise between performance and power usage. For mobile computers running on battery power, the greater the power usage, the shorter the battery life. To maximize battery life, Windows 7 provides different power plans and switches between them automatically when a computer is plugged in or running on battery.

However, the default battery power plan can reduce performance. To set the power plan manually, perform these steps:

1. Click the power icon in the system tray, and then click More Power Options.
2. Click Change Plan Settings.
3. Click Change Settings That Are Currently Unavailable.
4. Change the display and sleep settings for times when the computer is plugged in or running on battery.
5. To change other settings, click Change Advanced Power Settings. Adjust the settings, and then click OK. Some of the more useful performance-related settings include:
   - **Turn Off Hard Disk After** Windows can turn the hard disk off to save power if it is not used for a specific amount of time. Realistically, though, applications continue to use the hard disk even if the user is not actively working with the computer.
   - **Wireless Adapter Settings** Wireless adapters can use a significant amount of battery power because they must transmit and receive radio signals. By default, Windows 7 enables power saving for wireless connections when running on battery power. If wireless performance significantly decreases while on battery power, you can change the power saving mode to Maximum Performance while on battery power.
   - **Sleep** In Windows Vista and Windows 7, Sleep is a power-saving mode that combines both *Standby* (a low-power state that allows the computer to recover in a few seconds) and *Hibernation* (a zero-power state that stores the computer's memory to disk, but takes longer to recover). By default, Sleep in Windows 7 initially enters Standby mode and then enters Hibernation 20 minutes later. Adjust this setting to change that default.
   - **USB Settings** USB devices draw power from a computer. With USB selective suspend, Windows 7 can reduce the power usage of some USB devices. By default, USB selective suspend is enabled while Windows 7 is on battery power.
   - **Power Buttons And Lid** By default, Windows 7 automatically enters sleep mode when the lid of a mobile computer is closed. You can change this setting and configure how the power button functions.
   - **PCI Express** Some mobile computers have a PCI Express interface. This setting configures the power savings mode used for the PCI Express interface when on battery power or plugged in.
   - **Processor Power Management** Most modern processors can run at different speeds depending on the current processing requirements. When less processor time is needed, the processor runs slower, requiring less power. You can use these settings to change the minimum and maximum speed of the processor.

- **Multimedia Settings** You can use this setting to adjust video quality when on battery power. Enabling a higher video quality increases battery usage.
- **Battery** Adjust how Windows responds when a battery begins to run out of power.

6. Click Save Changes.

System Configuration

Troubleshooting often involves experimentation. For example, when troubleshooting a performance problem, you might stop a program or service from starting automatically and then test the computer to determine if the performance problem has been resolved. The challenge with this, however, is that you might disable useful applications and services not related to the problem.

The System Configuration Utility (Msconfig.exe) allows you to disable startup programs and system services individually or several at a time. Once you identify the source of the problem, you can easily re-enable the startup programs and services. To disable a startup program or service by using the System Configuration Utility, use these steps:

1. Click Start, type **msconfig**, and then press Enter.
2. To disable a service at startup, select the Services tab and clear the check box for the service.
3. To disable a startup program, select the Startup tab and clear the check box for the application.
4. Click OK. When prompted, click Restart.

   When Windows restarts, the changes you have made take effect.
5. When the computer restarts, determine whether your changes improved the computer's performance. If disabling the startup program or service did solve the problem, you can investigate it further. If there was no benefit, use the System Configuration utility to re-enable the startup program or service.

You can remove a startup program permanently using Control Panel. To prevent a service from starting automatically, use the Services console.

Quick Check

1. **Which tool would you use to adjust the processor affinity of a process, and why would you adjust it?**
2. **On which volume does Windows 7 store virtual memory by default?**

Quick Check Answers

1. **Task Manager. You would adjust processor affinity to limit the processor cores a process can run on.**
2. **On the system volume.**

PRACTICE Collect and Analyze Performance Data

In this practice, you collect performance data using a data collector set and then analyze it using a report and Performance Monitor.

EXERCISE 1 Perform System Diagnostics

In this exercise, you collect performance data by using a built-in data collector set.

1. Click Start, right-click Computer, and then click Manage.
2. In the Computer Management console, expand System Tools, Performance, Data Collector Sets, and then System.
3. Right-click System Diagnostics, and then click Start. Notice that a green arrow appears on the System Diagnostics icon.
4. While the System Diagnostics data collector set is running, click System Diagnostics. Browse through the various data collectors. In particular, view the properties of the following data collectors:
   - Performance Counter
   - NT Kernel
   - Operating System
   - UAC Settings
   - Windows Update Settings
5. The green arrow disappears from the System Diagnostics icon after the data collector set has finished running in one minute. Now, right-click System Diagnostics, and click Latest Report.
6. Examine the Diagnostic Results section and investigate any error or warning conditions. Then, investigate each of the other sections of the report to identify the following pieces of information:
   - Processor utilization
   - The number of processors and whether the processors are hyperthreaded or not
   - Memory utilization
   - Total physical memory
   - Whether the operating system architecture is 32-bit or 64-bit
   - The name of the workgroup or domain the computer is a member of
   - The name of the anti-spyware, antivirus, and firewall software installed, if any
   - Whether User Access Control (UAC) is enabled
   - Whether the Computer Browser, Server, Workstation, and Windows Update services are running
   - Which service is using the most processor time

- Whether IRQ 3 is in use
- The Windows Experience Index rating for the processor, memory, and hard disk
- Basic input/output system (BIOS) type and version
- The Internet Protocol (IP) address that is sending the most bytes to the local computer
- The number of IPv4 and IPv6 connections
- The file causing the most disk input/output (I/O)
- The application with the largest working set

EXERCISE 2 Create a Performance Graph

In this exercise, you use Performance Monitor to analyze graphically the data you gathered in Exercise 1.

1. In the Computer Management console, select the System Tools\Performance\Monitoring Tools\Performance Monitor node.
2. Click the View Log Data button on the toolbar to open the Source tab of the Performance Monitor Properties dialog box.
3. Select Log Files. Then, click Add. Select the C:\Perflogs\System\Diagnostics*<Computer_Name>_yyyymmdd-######*\Performance Counter.blg file to open the performance counter log created when you ran the System Diagnostics data collector set. Click Open.
4. Click OK to return to Performance Monitor.

   Now you are viewing the logged performance data. However, because you have not added any counters to the chart, nothing is visible.
5. Click the Add button on the toolbar. Add the following counters to the chart, and then click OK:
   - IPv4\Datagrams/sec
   - IPv6\Datagrams/sec
   - Memory\% Committed Bytes In Use
   - PhysicalDisk\Disk Bytes/sec
   - Processor\% Processor Time
   - System\Processes
6. Press Ctrl+H to highlight the selected counter. Browse through the available counters and examine their performance during the one minute log period.
7. Drag your mouse horizontally across the middle of the chart to select about 30 seconds of the chart. Then, right-click the chart and click Zoom To. Notice that the chart displays a smaller period of time.
8. Use the slider below the chart to select the entire chart time period. Then, right-click the chart and click Zoom To.

EXERCISE 3 Disable a Service Temporarily with the System Configuration Utility

In this exercise, you temporarily disable a service with the System Configuration utility.

1. Click Start, type **msconfig**, and then press Enter.
2. In the System Configuration Utility dialog box, on the Services tab, clear the check box next to the Computer Browser service.
3. Click OK.
4. In the System Configuration dialog box, click Restart. Windows restarts.
5. Log back on to Windows. Click Start, type **msconfig**, and then press Enter.
6. On the Services tab, is the Computer Browser service stopped or started?

   Stopped.
7. Select the check box next to the Computer Browser service, and then click OK.
8. In the System Configuration dialog box, click Restart.

Lesson Summary

- Task Manager provides a quick way to examine a computer's performance and solve some performance problems. With Task Manager, you can identify which processes are consuming the most resources and either lower the priority of those processes or end them.
- You can use Performance Monitor to analyze system statistics in real time or you can use it to analyze data logged using a data collector set.
- Data collector sets and reports gather performance and configuration data about a computer and enable you to analyze that information easily using reports or Performance Monitor.
- Disk performance problems are most often caused by low disk space and fragmentation. Windows 7 automatically defragments disks that need it, but if disk space is too low, some fragmentation occurs anyway. To free up wasted disk space, you can use the Disk Cleanup tool.
- If a startup program is causing performance problems, you can use the System Configuration (Msconfig.exe) tool to prevent it from starting. The System Configuration tool provides a convenient way to re-enable applications if you later determine that they are not the source of the problem.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Troubleshooting Performance Problems." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE **ANSWERS**

Answers to these questions and explanations of why each answer choice is correct or incorrect are located in the "Answers" section at the end of the book.

1. You are a systems administrator for an enterprise company. A user calls to complain that his computer is responding very slowly, and that Microsoft Office Word is not responding. He has attempted to close Word, but it has not stopped. What can you do?
   - **A.** Press Ctrl+Alt+Del, and then click Start Task Manager. On the Applications tab, click Word, and then click End Task.
   - **B.** Press Ctrl+Alt+Del, and then click Start System Configuration Utility. On the Startup tab, click Microsoft Word, and then click OK.
   - **C.** Press Alt+Tab, and then click Start Task Manager. On the Applications tab, click Word, and then click End Task.
   - **D.** Press Alt+Tab, and then click Start System Configuration Utility. On the Startup tab, click Microsoft Word, and then click OK.
2. Which of the following factors most increases disk fragmentation?
   - **A.** Running from battery power
   - **B.** A large paging file
   - **C.** Low free disk space
   - **D.** Using a flash drive
3. Which of the following performance problems might occur on a mobile computer using battery power? (Choose all that apply.)
   - **A.** Increased use of virtual memory
   - **B.** Slower memory access
   - **C.** Slower wireless networking
   - **D.** Lower-quality video

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can perform the following tasks:

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenarios. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- The Windows 7 event log contains a great deal of valuable information, including events that describe problems that have already occurred or might occur soon. By monitoring these events using event forwarding, you can respond to problems more quickly or prevent them from becoming critical.
- Using Task Manager, Performance Monitor, and data collector sets, you can identify the cause of performance problems quickly. Task Manager can even solve some performance problems by changing the priority of a running process or closing an application. If a startup program or service seems to be causing the performance problem, use the System Configuration tool to disable different programs temporarily during troubleshooting.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- **Collecting computer**
- **Event forwarding**
- **Forwarding computer**
- **Hibernation**
- **Listener**
- **Pull delivery mode**
- **Push delivery mode**
- **Standby**

Case Scenarios

In the following case scenarios, you apply what you've learned about subjects of this chapter. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Monitoring Kiosk Computers

You are a systems administrator at the Baldwin Museum of Science. In addition to managing computers used by internal staff, you manage several computers running Windows Vista that are configured as kiosks in the museum's front lobby. Visitors to the museum can use these computers to browse a limited number of Web sites with science-related content. Desktop security restrictions limit the applications that users can run and the Web sites they can visit.

The museum attracts a large audience of intelligent, computer-savvy visitors. Unfortunately, some of them have taken it as a challenge to break into the kiosk computers. For example, you recently happened upon an attacker using an internal wireless connection to attack a kiosk computer across the network. You noticed the attack because you happened to discover an event in the event log, as shown in Figure 8-12.

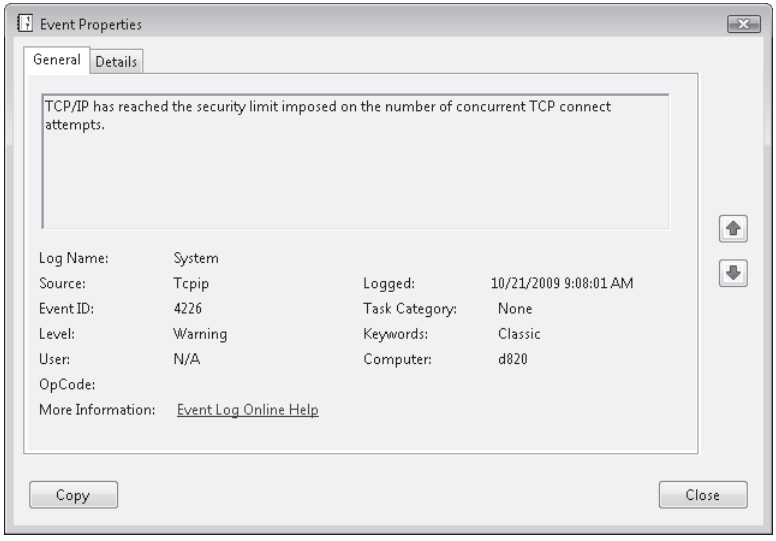

FIGURE 8-12 An event indicating an active attack in your organization

Questions

Answer the following questions for your manager:

1. You manage several kiosk computers. How can you monitor all their event logs easily to check for this particular event?
2. Which bandwidth optimization technique should you use for event forwarding?
3. If this event appears, you need to know about it immediately. How can you be actively notified of an attack?

Case Scenario 2: Troubleshooting a Performance Problem

You are the lead systems administrator at Woodgrove Bank. Several times a day your organization's IT support staff receives support requests from users who are experiencing a slow computer. However, the support staff has been unable to identify the cause of the performance problem, and resolves the problem by having the users restart their computer.

Interviews

Following is a list of company personnel interviewed and their statements:

- **Stuart Railson, Desktop Support Technician** "These users are so hard to help. This guy complained that his computer was slow, and he has this attitude like it's my fault. I think the cause of the problem is that the computer is too old. We should upgrade the processor or memory or something. I just have the users restart the computer. I think more users experience the slowdowns than actually call us, but they've figured out that they should just restart the computer to fix it."
- **Angela Barbariol, IT Manager** "As you know, all our computers are running Windows 7 with modern, dual-core processors and at least 3 GB of RAM. For the types of applications these users run, that should be plenty. Proof of this is that the computers perform fine when they're initially restarted. Frankly, I'm embarrassed that we've been solving the problem by restarting the computers because that interrupts user productivity. Let's find the source of the performance problems so we can fix them."

Questions

Answer the following questions for your manager:

1. Which tools would you use to identify the source of the problem? How would you use those tools?
2. What do you think the problem might be? Why would restarting the computer fix it temporarily?

Suggested Practices

To help you master the exam objectives presented in this chapter, complete the following tasks.

Identify and Resolve Performance Issues

For this task, you should complete at least Practices 1 and 2 to gain more experience with event forwarding. If you want a better understanding of how to configure event forwarding in an enterprise, complete Practice 3 as well. Completing these configuration tasks also helps you with your troubleshooting skills because problems are bound to arise when configuring non-default event forwarding.

Next, complete Practices 4 through 7 to get more experience monitoring computer performance. Finally, complete Practice 8 to get a better understanding of how much real-world disk space is wasted.

- **Practice 1** Configure a workgroup computer to forward events to another workgroup computer.
- **Practice 2** Configure a forwarding computer to send events to a collecting computer using each of the three standard bandwidth optimization techniques. Then, customize the event forwarding configuration by reducing the time required to forward events by half.
- **Practice 3** Use Group Policy to configure multiple client computers to forward events to a collecting computer. For the greatest scalability, use logon scripts to configure the forwarding computers—it would be too time-consuming to configure forwarding computers manually in an enterprise.
- **Practice 4** Run both standard data collector sets on several production computers. Analyze the report generated by each.
- **Practice 5** Leave the Performance of Task Manager open while you do other work on your computer. If you see utilization increase, use the Processes tab to identify the process causing the extra utilization. Repeat this practice with the Networking tab.
- **Practice 6** Start an application, such as Notepad, and then end the process using the Processes tab of Task Manager.
- **Practice 7** In Performance Monitor, add the Network Interface\Bytes Total/sec counter for your primary network interface. Then, copy a file across the network. Make note of the maximum bytes per second. Multiply that value times eight to determine the maximum bandwidth used in bits per second. What percentage of the total network bandwidth did the file transfer use?
- **Practice 8** Run the Disk Cleanup tool on several production computers. How much space are you able to free, on average?

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just one exam objective, or you can test yourself on all the 70-685 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **PRACTICE TESTS**

For details about all the practice test options available, see the section entitled "How to Use the Practice Tests," in the Introduction of this book.