EXAM CRAM

The Smart Way to Study™

Exam 70-622

MCITP

Supporting and Troubleshooting Applications on a Windows Vista® Client for Enterprise Support Technicians

Paul A. Mancuso
David R. Miller

MCITP 70-622 Exam Cram: Supporting and Troubleshooting Applications on a Windows Vista® Client for Enterprise Support Technicians

ISBN-13: 978-0-7897-3719-9

ISBN-10: 0-7897-3719-1

Library of Congress Cataloging-in-Publication Data

Mancuso, Paul.

MCITP 70-622 exam cram / Paul Mancuso, David Miller.

p. cm.

ISBN 978-0-7897-3719-9 (pbk. w/cd)

1. Electronic data processing personnel—Certification. 2. Microsoft software—Examinations—Study guides. 3. Microsoft Windows (Computer file) I. Miller, David. II. Title.

QA76.3.M3245 2008

005.4'46—dc22

2008016537

Printed in the United States of America

First Printing: May 2008

Associate Publisher
David Dusthimer

Executive Editor
Betsy Brown

Development Editor
Box Twelve Communications, Inc.

Technical Editors
Chris Crayton
Pawan Bhardwaj

Managing Editor
Patrick Kanouse

Project Editor
Seth Kerney

Copy Editor
Chuck Hutchinson

Indexer
WordWise Publishing, Inc.

Proofreader
Kathy Ruiz

Publishing Coordinator
Vanessa Evans

Book Designer
Gary Adair

Page Layout
TnT Design, Inc.

Introduction

Welcome to the *70-622 Exam Cram!* Whether this book is your first or 15th *Exam Cram* series book, you'll find information here to help ensure your success as you pursue knowledge, experience, and certification.

This book aims to help you get ready to take and pass the 70-622 exam. After you pass this exam, along with the 70-620 exam, you will earn the Microsoft Certified Information Technology Professional (MCITP): Enterprise Support Technician certification.

This introduction explains Microsoft's certification programs in general and describes how the *Exam Cram* series can help you prepare for Microsoft's latest certification exams. Chapters 1 through 5 cover the information you need to know to pass the 70-622 certification exam. The two sample tests at the end of the book should give you a reasonably accurate assessment of your knowledge and, yes, we've provided the answers and their explanations for these sample tests. Read the book, understand the material, and you stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass Microsoft certification exams. *Exam Cram* books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, we streamline and highlight the pertinent information by presenting and dissecting the questions and problems we discovered that you're likely to encounter on a Microsoft test.

Nevertheless, if you want to completely prepare yourself for any Microsoft test, we recommend that you begin by taking the self-assessment included in this book, immediately following this introduction. The self-assessment tool helps you evaluate your knowledge base against the requirements for becoming a Microsoft Certified Technology Specialist (MCTS) and is the first step in earning more advanced certifications, including the Microsoft Certified IT Professional (MCITP), Microsoft Certified Professional Developer (MCPD), and Microsoft Certified Architect (MCA).

Based on what you learn from the self-assessment, you might decide to begin your studies with classroom training or some background reading. On the other hand, you might decide to pick up and read one of the many study guides available from Microsoft or third-party vendors. We also recommend that you supplement your study program with visits to http://www.examcram.com to receive additional practice questions, get advice, and track the Windows certification programs.

This book also offers you an added bonus of accessing *Exam Cram* practice tests online. All you need is a connection to the Internet, and you can take advantage of these practice exam questions directly from your own web browser! This software simulates the Microsoft testing environment with similar types of questions that you're likely to see on the actual Microsoft exam. We also strongly recommend that you install, configure, and play around with the Microsoft Windows Vista operating system. Nothing beats hands-on experience and familiarity when it comes to understanding the questions you're likely to encounter on a certification test. Book learning is essential, but without a doubt, hands-on experience is the best teacher of all!

The Value of Certification

It is an established fact that the field of computers and networking is a fast-paced environment. Therefore, employees who work in Information Technology (IT) must learn to keep up with the ever-changing technology and have the ability to learn new technology. It is said that IT professionals must be able to learn or retrain themselves every 1 to 1½ years.

According to *Certification Magazine* (http://www.certmag.com), the successful IT worker must

- Be proficient in two or more technical specialties.
- Be able to wear multiple hats.
- Be more business-oriented because hiring managers are looking for employees who see the big picture of profit, loss, competitive advantage, and customer retention and understand that IT fits into this picture.
- Be able to work easily with nontechnical personnel.
- Have soft skills of good listening, problem solving, and effective written and verbal communication.

In addition, there is a demand for those who can demonstrate expertise in IT project management. Those moving to a mid- to high-level position will have a mix of academic credentials and industry certifications, as well as increasing levels of responsibility.

Today, technical certifications are highly valuable. Depending on which certification or certifications an individual has, they can allow that user to begin as an entry-level technician or administrator, or those certifications can demonstrate the knowledge and capabilities of a current technician or administrator. Technical

companies see some technical certifications as valuable as a college degree, and nontechnical companies see them just a little less than a college degree.

You can see that certification is

- A demonstration of specific areas of competence with particular technologies
- A credential desired or required by an increasing number of employers
- A tool people use successfully to challenge themselves
- A road map for continuing education
- A potential bridge to a new specialty
- Evidence that you are self-motivated and actively working to stay current

On the other hand, certification is not a substitute for extensive hands-on experience, and it is not a career cure-all. Lastly, being able to pass these exams usually takes a little bit of work and discipline.

The Microsoft Certification Program

Microsoft currently offers multiple certification titles, each of which boasts its own special abbreviation. (As a certification candidate and computer professional, you need to have a high tolerance for acronyms.)

The newer certifications based on Windows Vista and Windows Server 2008 are as follows:

- **Microsoft Certified Technology Specialist (MCTS)**—For professionals who target specific technologies and distinguish themselves by demonstrating in-depth knowledge and expertise in the various Microsoft specialized technologies. The MCTS is a replacement for the MCP program.
- **Microsoft Certified IT Professional (MCITP)**—For professionals who demonstrate comprehensive skills in planning, deploying, supporting, maintaining, and optimizing IT infrastructures. The MCITP is a replacement for the MCSA and MCSE programs.
- **Microsoft Certified Architect (MCA)**—For professionals who are identified as top industry experts in IT architecture that use multiple technologies to solve business problems and provide business metrics and measurements. Candidates for the MCA program are required to present to a review board—consisting of previously certified architects—to earn the certification.

For trainers and curriculum developers, the following certifications are available:

- **Microsoft Certified Trainer (MCT)**—For qualified instructors who are certified by Microsoft to deliver Microsoft training courses to IT professionals and developers.
- **Microsoft Certified Learning Consultant (MCLC)**—For recognized MCTs whose job roles have grown to include frequent consultative engagements with their customers and who are experts in delivering customized learning solutions that positively affect customer return on investment (ROI).

For the best place to keep tabs on all Microsoft certifications, you need to view the following website:

http://www.microsoft.com/learning/default.mspx

Because Microsoft changes its website often, this URL may not work in the future. Therefore, you should use the Search tool on the Microsoft site to find more information on a particular certification.

Microsoft Certified Technology Specialist (MCTS)

Technology Specialist certifications enable you to target specific technologies and distinguish yourself by demonstrating in-depth knowledge and expertise in your specialized technologies. Microsoft Certified Technology Specialists are consistently capable of implementing, building, troubleshooting, and debugging a particular Microsoft technology.

At the time of the writing of this book, there are 19 Microsoft Certified Technology Specialist (MCTS) certifications:

- Technology Specialist: Maintaining Projects with Microsoft Office Project 2007
- Technology Specialist: Enterprise Project Management with Microsoft Office Project Server 2007
- Technology Specialist: .NET Framework 2.0 Web Applications
- Technology Specialist: .NET Framework 2.0 Windows Applications
- Technology Specialist: .NET Framework 2.0 Distributed Applications
- Technology Specialist: SQL Server 2005

- Technology Specialist: SQL Server 2005 Business Intelligence
- Technology Specialist: BizTalk Server 2006
- Technology Specialist: Microsoft Office Live Communications Server 2005
- Technology Specialist: Microsoft Exchange Server 2007, Configuration
- Technology Specialist: Microsoft Office SharePoint Server 2007, Configuration
- Technology Specialist: Microsoft Office SharePoint Server 2007, Application Development
- Technology Specialist: Windows Mobile 5.0, Applications
- Technology Specialist: Windows Mobile 5.0, Implementing and Managing
- Technology Specialist: Windows Server 2003 Hosted Environments, Configuration, and Management
- Technology Specialist: Windows SharePoint Services 3.0, Application Development
- Technology Specialist: Windows SharePoint Services 3.0, Configuration
- Technology Specialist: Windows Vista and 2007 Microsoft Office System Desktops, Deploying and Maintaining
- Technology Specialist: Windows Vista, Configuration

Microsoft Certified IT Professional (MCITP)

The new Microsoft Certified IT Professional (MCITP) credential lets you highlight your specific area of expertise. Now, you can easily distinguish yourself as an expert in database administration, database development, business intelligence, or support. At the time of this writing, the following Microsoft Certified IT Professional certifications exist:

- IT Professional: Business Intelligence Developer
- IT Professional: Consumer Support Technician
- IT Professional: Database Developer
- IT Professional: Database Administrator

- IT Professional: Enterprise Messaging Administrator
- IT Professional: Enterprise Project Management with Microsoft Office Project Server 2007
- IT Professional: Enterprise Support Technician
- IT Professional: Enterprise Administrator
- IT Professional: Server Administrator

At the time of this writing, details are just starting to be revealed on the Microsoft Certified Technology Specialist (MCTS) on Windows Server 2008. The MCTS on Windows Server 2008 will help you and your organization take advantage of advanced server technology with the power to increase the flexibility of your server infrastructure, save time, and reduce costs. Transition certifications are available today for Windows Server 2003 certified professionals, and full certification paths will be available soon after the Windows Server 2008 product release. For more details about these certifications, visit the following website:

http://www.microsoft.com/learning/mcp/windowsserver2008/default.mspx

If the URL is no longer available, don't forget to search for MCTS and Windows Server 2008 using the Microsoft search tool found on the Microsoft website.

Microsoft Certified Technology Specialist: Windows Vista, Configuration

The Microsoft Certified Technology Specialist certifications enable professionals to target specific technologies and distinguish themselves by demonstrating in-depth knowledge and expertise in their specialized technologies. A Microsoft Certified Technology Specialist in Windows Vista, Configuration possesses the knowledge and skills to configure Windows Vista for optimal performance on the desktop, including installing, managing, and configuring the new security, network, and application features in Windows Vista.

To earn the Microsoft Certified Information Technology Professional (MCITP): Enterprise Support Technician certification, you must pass two exams:

- Exam 70-620 TS: Microsoft Windows Vista Client, Configuring
- Exam 70-622 IT Pro: Supporting and Troubleshooting Applications on a Windows Vista Client for Enterprise Support Technicians

Exam 70-620 focuses on supporting end-user issues about network connectivity, security, and applications installation and compatibility, and logon problems that include account issues and password resets.

If you decide to take a Microsoft-recognized class, you can choose from two classes:

- Course 5115: Installing and Configuring the Windows Vista Operating System (3 days)
- Course 5116: Configuring Windows Vista Applications and Tools (2 days)

The preparation guide (including exam objectives) for Exam 70-620 TS: Microsoft Windows Vista, Configuring is available at

http://www.microsoft.com/learning/exams/70-620.mspx

Exam 70-622 focuses on IT professionals who typically work as Enterprise Support Technicians dealing with implementing, administering, and troubleshooting Windows Vista in an upper medium-sized organization or enterprise environment that uses Windows Vista.

If you decide to take a Microsoft recognized class, you can choose from two classes:

- Course 5118: Maintaining and Troubleshooting Windows Vista Computers (3 days)
- Course 5119: Supporting the Windows Vista Operating System and Applications (2 days)

The preparation guide (including exam objectives) for Exam 70-622 IT Pro: Supporting and Troubleshooting Applications on a Windows Vista Client for Enterprise Support Technicians is available at

http://www.microsoft.com/learning/exams/70-622.mspx

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take Exam 70-622 is (U.S.) $125, and if you don't pass, you can take the test again for an additional (U.S.) $125 for each attempt. In the United States and Canada, tests are administered by Thompson Prometric. Here's how you can contact the testing administrator:

Prometric—You can sign up for a test through the company's website, http://www.2test.com or http://www.prometric.com. Within the United States and Canada, you can register by phone at 800-755-3926. If you live outside this region, you should check the Prometric website for the appropriate phone number.

To sign up for a test, you must possess a valid credit card or contact Prometric for mailing instructions to send a check (in the United States). Only when payment is verified or a check has cleared can you actually register for a test.

To schedule an exam, you need to call the appropriate phone number or visit the Prometric website at least one day in advance. To cancel or reschedule an exam in the United States or Canada, you must call before 3 p.m. Eastern time the day before the scheduled test time (or you might be charged even if you don't show up to take the test). When you want to schedule a test, you should have the following information ready:

- Your name, organization, and mailing address.
- Your Microsoft test ID. (In the United States, this means your Social Security number; citizens of other countries should call ahead to find out what type of identification number is required to register for a test.)
- Your Microsoft Certified Professional (MCP) ID, if you have one.
- The name and number of the exam you want to take.
- A method of payment. (As mentioned previously, a credit card is the most convenient method, but alternate means can be arranged in advance, if necessary.)

After you sign up for a test, you are told when and where the test is scheduled. You should arrive at least 15 minutes early. You must supply two forms of identification, one of which must be a photo ID to be admitted into the testing room.

Tracking Certification Status

As soon as you pass your first qualified Microsoft exam and earn a professional certification, Microsoft generates a transcript that indicates which exams you have passed. You can view a copy of your transcript at any time by going to the MCP secured site at https://mcp.microsoft.com/mcp (this site may change as the MCP certification is retired), and selecting the Transcript Tool. This tool enables you to print a copy of your current transcript and confirm your certification status.

After you pass the necessary set of exams, you are certified. Official certification is normally granted after six to eight weeks, so you shouldn't expect to get your credentials overnight. The package for official certification that arrives includes a Welcome Kit that contains a number of elements (see the Microsoft website for other benefits of specific certifications):

- A certificate that is suitable for framing, along with a wallet card and lapel pin.
- A license to use the related certification logo, which means you can use the logo in advertisements, promotions, and documents and on letterhead, business cards, and so on. Along with the license comes a logo sheet, which includes camera-ready artwork. (Note that before you use any of the artwork, you must sign and return a licensing agreement that indicates you'll abide by its terms and conditions.)
- Access to the *Microsoft Certified Professional Magazine Online* website, which provides ongoing data about testing and certification activities, requirements, changes to the MCP program, and security-related information on Microsoft products.

Many people believe that the benefits of MCP certification go well beyond the perks that Microsoft provides to newly anointed members of this elite group. We're starting to see more job listings that request or require applicants to have Microsoft and other related certifications, and many individuals who complete Microsoft certification programs can qualify for increases in pay and responsibility. As an official recognition of hard work and broad knowledge, a certification credential is a badge of honor in many IT organizations.

About This Book

Each topical *Exam Cram* chapter follows a regular structure and contains graphical cues about important or useful information. Here's the structure of a typical chapter:

- **Opening hotlists**—Each chapter begins with a list of the terms, tools, and techniques that you must learn and understand before you can be fully conversant with that chapter's subject matter. The hotlists are followed by one or two introductory paragraphs to set the stage for the rest of the chapter.
- **Topical coverage**—After the opening hotlists and introductory text, each chapter covers a series of topics related to the chapter's subject.

Throughout each chapter, we highlight topics or concepts that are likely to appear on a test, using a special element called an Exam Alert:

EXAM ALERT

This is what an Exam Alert looks like. Normally, an alert stresses concepts, terms, software, or activities that are likely to relate to one or more certification-test questions. For that reason, we think any information in an alert is worthy of unusual attentiveness on your part.

You should pay close attention to material flagged in Exam Alerts; although all the information in this book pertains to what you need to know to pass the exam, Exam Alerts contain information that is really important. You'll find what appears in the meat of each chapter to be worth knowing, too, when preparing for the test. Because this book's material is condensed, we recommend that you use this book along with other resources to achieve the maximum benefit.

In addition to the alerts, we provide tips to help you build a better foundation for Windows Vista knowledge. Although the tip information might not be on the exam, it is certainly related and will help you become a better-informed test taker.

TIP

This is how tips are formatted. Keep your eyes open for these, and you'll become a Windows Vista guru in no time!

NOTE

This is how notes are formatted. Notes direct your attention to important pieces of information that relate to Windows Vista and Microsoft certification.

- **Exam prep questions**—Although we address test questions and topics throughout the book, the section at the end of each chapter presents a series of mock test questions and explanations of both correct and incorrect answers.
- **Details and resources**—Every chapter ends with a section titled "Need to Know More?" This section provides direct pointers to Microsoft and third-party resources that offer more details on the chapter's subject. In addition, this section ranks or at least rates the quality and thoroughness

of the topic's coverage by each resource. If you find a resource you like in that collection, you should use it, but you shouldn't feel compelled to use all the resources. On the other hand, we recommend only resources that we use on a regular basis, so none of our recommendations will be a waste of your time or money (but purchasing them all at once probably represents an expense that many network administrators and Microsoft certification candidates might find hard to justify).

The bulk of the book follows this chapter structure, but we'd like to point out a few other elements. The two practice exams provide good reviews of the material presented throughout the book to ensure that you're ready for the certification exam.

Finally, the tear-out Cram Sheet attached next to the inside front cover of this *Exam Cram* book represents a condensed collection of facts and tips that we think are essential for you to memorize before taking the test. Because you can dump this information out of your head onto a sheet of paper before taking the exam, you can master this information by brute force; you need to remember it only long enough to write it down when you walk into the testing room. You might even want to look at the Cram Sheet in the car or in the lobby of the testing center just before you walk in to take the exam.

We've structured the topics in this book to build on one another. Therefore, some topics in later chapters make the most sense after you've read earlier chapters. That's why we suggest that you read this book from front to back for your initial test preparation. If you need to brush up on a topic or if you have to bone up for a second try, you can use the index or table of contents to go straight to the topics and questions that you need to study. Beyond helping you prepare for the test, this book is useful as a tightly focused reference to what we think are some of the most important aspects of Windows Vista.

The book uses the following typographical conventions:

- Command-line strings that are meant to be typed into the computer are displayed in monospace text, such as

```
net use lpt1: \\print_server_name\printer_share_name
```

- *New terms* are introduced in italics.

Given all the book's elements and its specialized focus, we've tried to create a tool to help you prepare for and pass Microsoft Exam 70-622. Please share with us your feedback on the book, especially if you have ideas about how we can improve it for future test takers. Send your questions or comments about this book via

email to feedback@quepublishing.com. We'll consider everything you say carefully, and we'll respond to all suggestions. For more information on this book and other Que Certification titles, visit our website at http://www.quepublishing.com. You should also check out the new *Exam Cram* website at http://www.examcram.com, where you'll find information updates, commentary, and certification information.

Thanks for making this *Exam Cram* book a pivotal part of your certification study plan. Best of luck on becoming certified!

CHAPTER 3

Managing and Maintaining Systems That Run Windows Vista

Terms you'll need to understand:

- ✓ Active Directory (AD)
- ✓ Active Directory Users and Computers (ADUC)
- ✓ Local Computer Policy (LCP)
- ✓ Group Policy Object (GPO)
- ✓ AD Site
- ✓ AD Domain
- ✓ Organizational Unit (OU)
- ✓ L-S-D-OU-OU-OU
- ✓ Block Inheritance
- ✓ No Override/Enforced
- ✓ Group Policy Management Console (GPMC)
- ✓ Task Scheduler
- ✓ Event Viewer
- ✓ Event Subscriptions
- ✓ Windows Remote Management Service (WinRM)
- ✓ Windows Event Collector Utility (`wecutil.exe`)
- ✓ Reliability and Performance Monitor
- ✓ Data Collector Set

Techniques you'll need to master:

- ✓ Install and use the Group Policy Management Console
- ✓ Create, deploy, and troubleshoot Group Policy Objects (GPOs)
- ✓ Understand GPO processing
- ✓ Implement a Loopback GPO
- ✓ Implement an audit policy
- ✓ Implement a software deployment GPO
- ✓ Implement Device Restrictions by GPO
- ✓ Implement Software Restrictions by GPO
- ✓ Perform Resultant Set of Policies/Planning and Logging
- ✓ Schedule tasks with different triggers
- ✓ Understand Event Viewer
- ✓ Configure Event Forwarding from multiple Source computers to one Collector computer
- ✓ Configure Data Collector Sets in Performance Monitor

The tools that you must be familiar with and use in the management of Windows Vista computers in the enterprise are

- Active Directory Users and Computers (ADUC)
- Group Policy Management Console (GPMC)
- Group Policy Objects (GPO)
- Task Scheduler
- Event Viewer
- Reliability and Performance Monitor

As an enterprise support technician, you are responsible for management and maintenance of computers that run Windows Vista in the Enterprise. Your "heavy guns" in this administrative task are the *Group Policy Objects (GPOs)*. You need to be fluent with their settings, the way they get processed, and the implementation and troubleshooting of GPOs in your enterprise environment.

The exam tests your knowledge of what settings are available, where to link the GPO, how to have the GPO apply to only selected computers or users, and how to troubleshoot them when you aren't getting what you expected from the GPOs.

Another tool that you use is the *Task Scheduler*. This tool launches tasks at a later and perhaps regularly scheduled time. This tool has changed significantly since the last versions of the Windows operating system.

There is impressive new capability in the *Event Viewer*. You probably won't even recognize it from earlier versions. It has a powerful, customizable filter that allows you to capture events of about any nature you can imagine. In addition to this capability, you can now aggregate events from remote computers onto a single monitoring system, through the use of Event Forwarding to an Event Collector and subscription services.

Finally, you look at the new and improved *Reliability and Performance Monitor*, where you configure counters to view and log performance parameters on the local and on remote computers. This new tool includes a collection of objects and counters to monitor a large number of system resources.

You can configure many of the configuration parameters in the *Local Computer Policy (LCP)* on each client computer that runs Windows Vista. In the corporate enterprise, remember that these numerous configuration settings can and typically should be centrally managed and deployed by GPOs within the Active Directory structure.

Some exam questions address a standalone Windows Vista computer, whereas others address the Windows Vista computer within an Active Directory environment. You need to know what security settings are available and how these controls affect the behavior of the Windows Vista computer in both cases. So put on your seatbelts and read on carefully.

Group Policy Object Overview

Policies are the way that computers are managed, either standalone computers or computers in the enterprise. Policies establish the vast majority of the configuration settings that control how the computer boots up and then how your desktop environment is constructed when you log on.

The Standalone Computer

Each computer has a Local Computer Policy, or LCP (also referred to as the *Local GPO* or *LGPO*), that is made up of many configuration settings on the various configuration dialog boxes throughout the user interface, as well as numerous settings that are configurable only in a Microsoft Management Console (MMC) called the Local Computer Policy. This policy is stored in the Registry on the computer's hard drive and is applied every time the computer is booted up. This computer configuration from the Local Computer Policy gets read into random access memory (RAM) on the computer. Think of this RAM copy of the Registry as the live, awake brain of the computer when it is booted up. This RAM copy of computer settings from the Registry is in place when you are presented with the Windows Graphical Identification aNd Authentication (GINA) dialog box.

Further configuration for the desktop environment is controlled by configuration parameters stored within your user profile in a file called `NTUSER.DAT`. `NTUSER.DAT` gets read into RAM from your profile folder when you successfully log on to the computer. As you make changes to your desktop environment, like the desktop wallpaper or items on the Start menu, these changes get recorded in the RAM copy of `NTUSER.DAT`. When you log off, by default, the operating system saves these changes into your profile. This file is the primary source of the configuration parameters that define your desktop environment.

The first time you log on to a computer, the operating system copies a read-only and hidden folder under `C:\Users` called `\Default` to a new folder under `C:\Users` and renames the new folder with your logon name. Within that folder is the file named `NTUSER.DAT`. This becomes your user profile on this specific computer. After that first logon on a given computer, now that you have an existing profile, this existing copy of `NTUSER.DAT` is the one that gets read into RAM for your user profile.

To summarize, two components define a desktop environment on a standalone computer (not participating within an Active Directory environment): the configuration parameters in the Local Computer Policy and the configuration parameters in your user profile. They get applied in that order.

The LCP can be accessed on a Windows Vista computer by building it into a new MMC.

Building a Local Computer Policy (LCP)

To build the Local Computer Policy (LCP) MMC, follow these steps:

1. Click **Start > Run**, type **MMC**, and click **OK**. (You can also use **Start > Start Search > MMC** and then press **Enter**.)
2. From the menu, select **File > Add / Remove Snap-in**.
3. Select **Group Policy Object snap-in** and click **Add**.
4. Accept the Group Policy Object for the Local Computer by clicking **Finish**.
5. Click **OK**.
6. From the menu, select **File > Save As**.
7. Type **LCP.msc** and save the MMC either on the desktop or in Administrative Tools.

The Domain Member Computer

Back in the old days of the Windows NT domain and Windows 95 clients, Microsoft used something called *System Policies*, built using a tool called the System Policy Editor, to manage and configure these down-level computers. These System Policies would "tattoo" the Registry of the local box, actually writing settings to the Registry files on the local hard drive. If you wanted to remove policy settings from the computers, you had to write a new System Policy that would actually reverse the settings from the policy that was being removed.

When Windows 2000 was released, Microsoft implemented a whole new generation of policies and completely overhauled how they were applied on computers. These policies were improved yet again with the release of Windows XP, Windows Server 2003, and now again with Windows Vista. These new policies are called *Group Policy Objects*, or *GPOs*, and they exist in the Active Directory in

an enterprise environment. These policies get applied to the computer over the top of the Local Computer Policy and your user profile settings to provide enterprise administrative dominance over the local configuration settings.

NOTE

GPOs Apply to Domain Members Only Keep in mind that GPOs affect only computers and users that are members of an Active Directory domain. If the computer and user are not members of an AD domain, only the Local Computer Policy and the user's profile get applied to the user's desktop session. No GPOs. If you apply a GPO in AD and don't see the effects on the computer and user, double-check to be sure that the computer and user are members of the AD domain.

These new policies do not affect the configuration files on the hard drive (for the most part), so they do not "tattoo" the computer. Rather, as these new policies get applied, they modify the copy of the Registry (computer) and the profile (user) that has been read into RAM on the computer during the initial bootup and then the user logon for the current session. These modifications to settings do not get written back to the hard drive copies of the configuration files. Remember that this RAM copy is the actual functional copy that is being used to control and configure the user's current session.

L-S-D-OU-OU-OU

Active Directory (AD) is a database and a collection of directory services that support the database and the network operating system. AD is created by configuring one or more domain controllers on a network. AD utilizes four types of containers to store and organize AD objects, like computers and users:

- Forests
- Sites
- Domains
- Organizational Units

You can apply GPOs to sites, domains, and Organizational Units.

AD Forest

The *AD forest* is one or more AD domains that share a common schema. The schema is the structure of the AD database—not the data within the database, just the structure. The forest is created when you run `DCPromo` on a server to install your first domain controller in the first domain in the forest. This first

domain is referred to as the *forest root domain*. The name of this forest root domain also is the name of the forest. All domains within the forest are trusted by and trusting of all other domains within the forest. Therefore, since members of your forest are, by default, all trusted and trusting, a lack of trust with some new domain indicates the need to generate a second forest, or create the new, untrusted domain in a different, existing forest. Forests are logical containers and have no real connection to any physical location, other than you must place your domain controllers somewhere. GPOs cannot be linked to the forest.

AD Sites

AD sites are created in AD once the forest is established and are defined as a collection of well-connected segments, where the bandwidth is at least local area network (LAN) speed. LAN speed is currently considered to be 10Mbps or greater. Any network link between segments that drops below LAN speed is defined as a boundary of the site and indicates the need for the creation of an additional site. Because sites are defined by physical connectivity, they are considered to be physical containers, with one site per location that is connected to AD by slower links. There are two major benefits to defining sites:

- Client computers within a site are preferentially directed to local (within the same site) resources.
- AD replication within the site happens without much regard for bandwidth consumption (because all segments are well connected at high bandwidth LAN speeds), but AD replication between sites, over slower wide area network (WAN) links, can be carefully controlled so as to avoid saturation of these lower bandwidth links. GPOs can be linked to sites.

AD Domains

AD domains are logical containers that are created within an AD forest. Domains (and AD) are created, and exist, on domain controllers. Domains in AD are security boundaries. In Windows Server 2003, they are defined by their unique namespace, like mobeer.com, buymeabeer.us, or boboville.com, as well as their single-password policy per domain. If you need a different namespace, you need another AD domain. If you need a different password policy for users, you need another AD domain. Domains are logical containers and can exist in multiple sites if placed in one or more domain controllers in more than one site. GPOs can be linked to the domain.

NOTE

Password Policies Password policies for domain users must be applied at the domain level.

Organizational Units (OUs)

Organizational Units (OUs) are logical containers that are created within an AD domain. They are designed to be used to organize computers and users for two purposes: to delegate administrative authority of groups of computers and users to different administrators, and to provide grouping of computers and users for the assignment of different Group Policy Objects (GPOs). OUs can be nested within another parent OU, so they create a hierarchical structure, like the one shown in Figure 3.1. GPOs can be linked to Organizational Units.

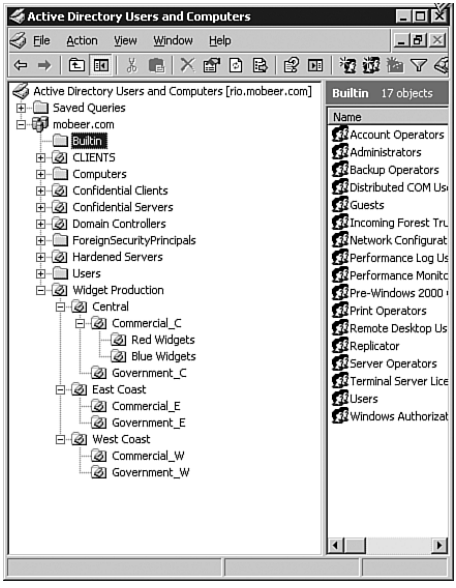

FIGURE 3.1 The hierarchical structure of OUs in an Active Directory domain.

The OU is represented in AD Tools by a folder with a book icon on it. A folder without a book icon on it is not an OU but is an AD container that cannot have GPOs linked to it. By default, AD provides only one OU called the *Domain Controllers OU* so that security-related GPOs can be applied to this most sensitive class of servers. Administrators must create all other OUs.

Policies are applied in the order of *L-S-D-OU-OU-OU*. That is the Local policy, then site policies, then domain policies, and finally OU policies, starting with the top-level OU, and then followed by its child OU, and then its child OU, and so on.

Policies have two halves:

- A computer half, called the *Computer Configuration*
- A user half, called the *User Configuration* (see Figure 3.2)

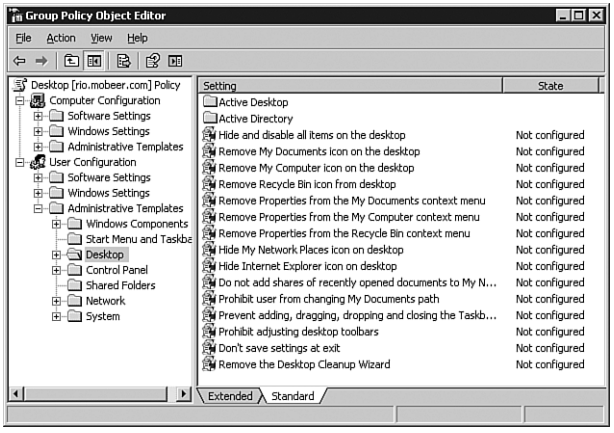

FIGURE 3.2 Group Policy Objects can be applied to computers and users.

Applying GPOs to a Computer and User in an AD Environment

GPOs are applied to a computer and user in an AD environment as follows.

The computer is turned on. All the Local settings are read from the files on the local hard drive that make up the Registry and the Local Computer Policy (LCP) and are placed in RAM. Again, think of this RAM copy of the Registry as the live, awake brain for this session on the computer. This is the "L" part of the computer boot-up process.

Because the computer is a member of Active Directory, it contacts a domain controller for its domain and authenticates its computer account with AD. It then compares its IP address to IP subnets configured in AD sites to identify which site the computer is currently in. The computer then downloads and reads all GPOs for the site that it is currently in and applies only the computer half of those GPOs to the RAM copy of the Registry on the computer. (At this point in the bootup process, it cannot apply the user portion because there is no way to know what user will eventually be logging on.) If any Site level settings conflict with any Local settings, the Site level settings override the Local settings. This is the "S" part of the computer bootup process.

The computer then downloads and reads all GPOs for the domain that it is a member of and applies only the computer half of those GPOs to the RAM copy of the Registry on the computer. By default, if any Domain level settings conflict

with any Local or Site level settings, the Domain level settings override the Local and Site level settings. This is the "D" part of the computer bootup process.

The computer then downloads and reads all GPOs for the top-level OU that its computer object resides in and applies only the computer half of those GPOs to the RAM copy of the Registry on the computer. By default, if any OU level settings conflict with any Local, Site, or Domain level settings, the OU level settings override the Local, Site, and Domain level settings. This is the "OU" part of the computer bootup process.

The computer repeats this process for each level OU that it may reside within. If the computer object for the computer resides in the top-level OU, these are the only OU GPOs to be processed. If the computer object for the computer resides in the third-level OU, the top-level OU GPOs are processed, then the second-level OU GPOs are processed, and finally the third-level OU GPOs are processed. By default, the last GPO that gets applied overrides all conflicts with previously applied GPOs.

Again, these GPO policies get applied to the computer over the top of the Local Computer Policy settings to provide enterprise (AD) administrative dominance over the local configuration settings.

When all appropriate OU GPOs are processed, the Windows GINA dialog box is presented, and finally you are allowed to attempt to log on.

You are prompted to press and hold the **Ctrl+Alt** keys and then press the **Del** key to initialize the logon process, as shown in Figure 3.3. You then provide your identity information, your username and password, and click **Enter**.

FIGURE 3.3 You provide your identity information, your username and password, and then click **Enter**.

When your identity information is accepted as valid by a domain controller, you are authenticated, and the L-S-D-OU-OU process begins all over again. Only this time it uses your user profile (L) and the user half of the S, D, and OU GPOs, as follows.

The user profile settings are read from the files on the local hard drive and are placed in RAM. This is the "L" part of the user logon process.

The computer again compares its IP address to IP subnets configured in AD sites to identify which site the computer is currently in. The computer then downloads and reads all GPOs for the site that it is currently in and applies only the user half of those GPOs to the RAM copy of the Registry on the computer. If any Site level settings conflict with any Local settings, the Site level settings override the Local settings. This is the "S" part of the user logon process.

The user object can be located in a different OU and even a different domain than the computer object, but because you are logging on to the computer, you must be in the same physical location as the computer and are subject to the computer's Site level GPOs.

The computer then contacts a domain controller for the domain that you are a member of and downloads and reads all GPOs for your domain. The computer applies only the user half of those GPOs to the RAM copy of the Registry on the computer. By default, if any Domain level settings conflict with any Local or Site level settings, the Domain level settings override the Local and Site level settings. This is the "D" part of the user logon process.

The computer then downloads and reads all GPOs for the top-level OU that the user account object resides in and applies only the user half of those GPOs to the RAM copy of the Registry on the computer. By default, if any OU level settings conflict with any Local, Site, or Domain level settings, the OU level settings override the Local, Site, and Domain level settings. This is the "OU" part of the user logon process.

The computer repeats this process for each level OU that the user account object may reside within. If the user account object resides in the top-level OU, these are the only OU GPOs to be processed. If the user account object for the computer resides in the third-level OU, then the top-level OU GPOs are processed, followed by the second-level OU GPOs, and finally the third-level OU GPOs are processed. By default, the last GPO that gets applied overrides all conflicts with previously applied GPOs.

Once again, these policies get applied to the RAM copy of the Registry on the computer over the top of the User Profile settings to provide enterprise (AD) administrative dominance over the local configuration settings.

Now you (finally) get your desktop and can begin working.

And If That Isn't Enough: Enforced, Block Inheritance, and Slow Link Detection

With all the different GPOs that can be applied to a computer and user, some settings in the different GPOs are bound to conflict. Suppose at the site level, a GPO sets the desktop wallpaper for all computers in the site to the company logo wallpaper. And then some domain administrator sets a GPO at the domain level so that the desktop wallpaper for all domain computers is a picture of the domain's softball team. By default, if any settings in the numerous GPOs conflict, the last GPO that gets applied wins the conflict.

This sounds like the lowliest administrator in charge of two or three computers and a few users in an OU can overrule the highest level enterprise administrator in charge of hundreds or thousands of computers and users. If left to the defaults, this is true. However, there is a setting called *Enforced* on each GPO. If this setting is enabled (it is *not* enabled by default), it locks every setting that is configured in the GPO, and no GPO that follows can override these locked settings. So with the Enforced setting enabled on GPOs, the first Enforced GPO that gets applied wins all conflicts. This is a top-down mechanism.

Another configurable setting regarding GPO processing is a bottom-up mechanism. If an administrator at a domain or some OU level does not want any previously applied, non-Enforced GPOs to affect his computers and users, he can enable a setting called *Block Inheritance* on the domain or the OU. This setting turns off processing of all GPOs from higher-level containers that are not Enforced. Remember, though, that a GPO with the Enforced setting enabled blows right past the Block Inheritance setting and is still processed by all computers and users in all child containers, even if the Block Inheritance setting is enabled.

One more parameter that changes the way GPOs are processed has to do with the bandwidth connecting the client computer to the domain controllers. Because some GPOs trigger a large amount of network traffic—a software deployment and folder redirection GPOs, for example—an evaluation of the bandwidth of the link to AD is performed before processing any GPOs. This is referred to as *Slow Link Detection*. If the link speed is below 500Kbps, the default data rate for a slow link, software GPOs do not deploy software, and folder redirection GPOs do not relocate folders. If a computer cannot identify the bandwidth of the link to AD, it assumes that it is using a slow link and may not process all appropriate GPOs, like the software deployment GPOs.

EXAM ALERT

In earlier versions of Windows, like Windows XP, the client computer utilized the Internet Control Message Protocol (ICMP) Echo Request, the same function used in the PING application, to perform the slow link detection process. This became problematic when we all began blocking ICMP Echo Requests on our firewalls, due to the numerous Denial of Service attacks that used it. Client computers began to fail to identify slow links, and therefore they would fail to process all appropriate GPOs because the firewalls on the domain controllers blocked their slow link detection mechanism, the ICMP Echo Request packets.

Windows Vista has solved this problem by using a different service to identify slow links. Windows Vista uses a service called *Network Location Awareness*, instead of ICMP, to perform Slow Link Detection so that all appropriate GPOs are processed by Windows Vista computers.

To ensure Windows XP computers process all appropriate GPOs, you might need to allow ICMP Echo Request packets through your firewalls.

GPO Refresh, Loopback GPO Processing, and Turning Off the "L"

A few settings within the GPO also can affect the way this GPO processing happens. The first one is called the *GPO Refresh*. GPOs are applied to the computer during its bootup and then to the user during logon. They also get reapplied on a regular interval to ensure that new GPOs take effect quickly.

By default, GPOs refresh on member servers, member client computers, and domain users every 90 minutes, plus a random offset of 0 to 30 minutes (90 to 120 minutes). GPOs refresh on domain controllers every 5 minutes and have no random offset. These default refresh intervals can be adjusted within the GPO to affect all future refresh intervals. You can make this adjustment under User Configuration > Administrative Templates > System > Group Policy for the user refresh, and under Computer Configuration > Administrative Templates > System > Group Policy for domain member servers, domain member client computers, and domain controllers, as shown in Figure 3.4.

EXAM ALERT

Remember that you can manually refresh GPOs by running the `gpupdate.exe /force` command on the target computer. The `/force` switch reapplies all applicable GPO settings.

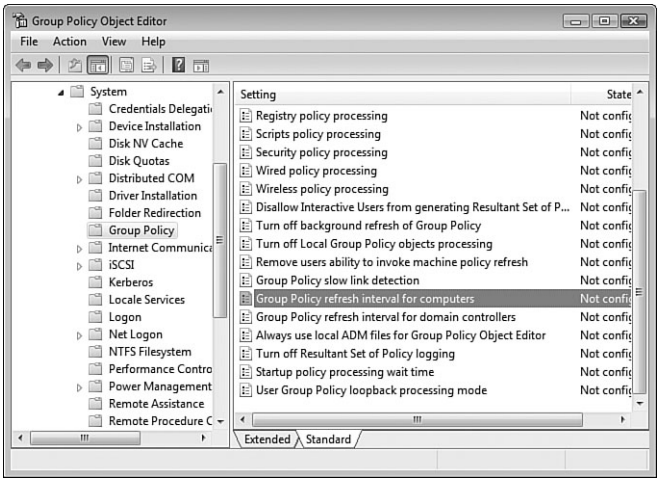

FIGURE 3.4 Determining the Group Policy refresh interval settings.

Another tool within a GPO that affects the way GPOs get processed is called *Loopback*, and it has two modes: Merge and Replace.

EXAM ALERT

You typically use Loopback when the computer is located in a public area, and you want to minimize or eliminate any User GPO settings that might be applied to the computer session.

With Loopback Merge mode enabled, after the GPO processing described earlier (L-S-D-OU-OU-OU for the computer and then L-S-D-OU-OU-OU again for the user) completes, Loopback Merge mode kicks in and reapplies the computer settings, just in case any user settings conflict with any computer settings. Remember, the last GPO that applies wins conflicts, by default. User GPOs apply after computer GPOs by default. Loopback reapplies the computer settings to win any conflicts with user settings.

With Loopback Replace mode enabled, after the GPO processing described earlier completes, Loopback Replace mode kicks in and reapplies the computer settings, just in case any user settings conflict with any computer settings. Then Loopback Replace mode throws away every user GPO setting that has been applied, and it processes the user half of all GPOs (S-D-OU-OU-OU) that apply to the computer's position in AD, not the user's position in AD. The Loopback processing GPO is shown in Figure 3.5.

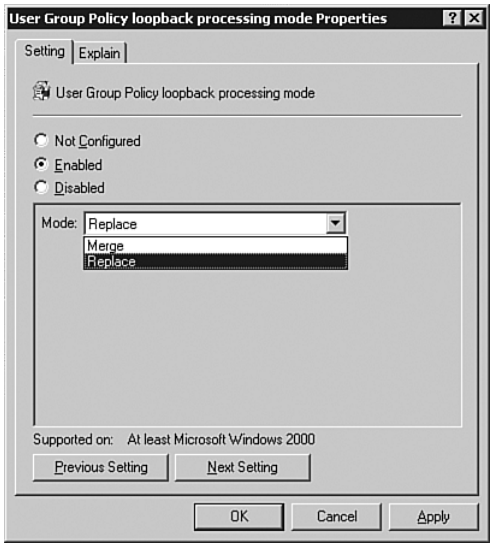

FIGURE 3.5 Using Loopback Merge mode or Loopback Replace mode to minimize or eliminate user GPO settings.

Another GPO setting that affects GPO processing is used to turn off Local Group Policy objects processing. You can access this setting under Computer Configuration\Administrative Templates\System\Group Policy in the Group Policy Management Console running on a Windows Vista computer, as shown in Figure 3.6.

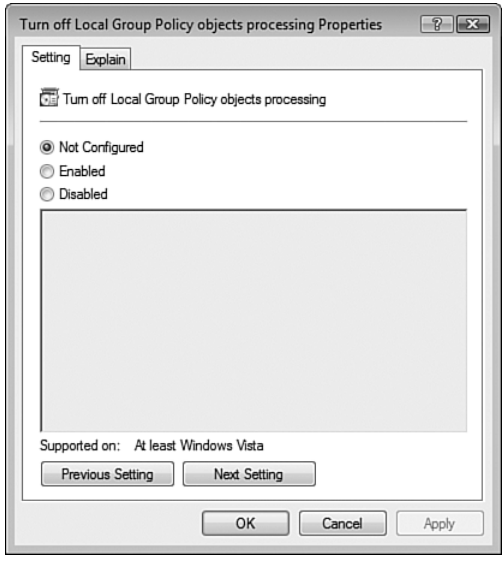

FIGURE 3.6 Disabling the processing of the Local Computer Policy.

EXAM ALERT

Enabling the Turn Off Local Group Policy Objects Processing GPO setting disables policy processing for the L part of L-S-D-OU and processes only S-D-OU.

NOTE

New GPOs There are approximately 800 new GPO settings exclusively for Windows Vista. You can access these new settings only by running GPMC and the Group Policy Object Editor (GPOE) on a Windows Vista computer. You cannot access these new Vista GPO settings from GPOE running on a Windows Server 2003 computer.

To be able to use and save the GPMC MMC on a Windows Vista computer, you must use a computer that is a member of an AD domain, and you must be logged in with a domain user account with sufficient privilege to create and edit GPOs.

You can access the *Group Policy Management Console (GPMC)*, as shown in Figure 3.7, on a Windows Vista computer by building a new MMC.

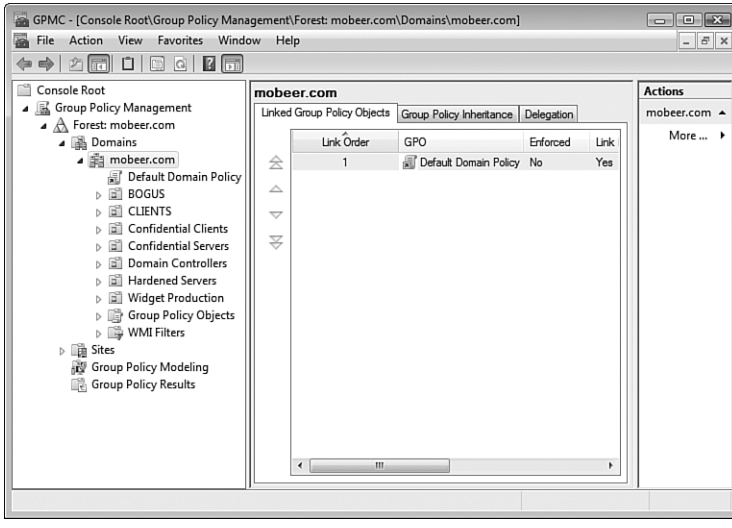

FIGURE 3.7 Accessing the Group Policy Management Console.

Building the Group Policy Management Console (GPMC) MMC

To build the Group Policy Management Console (GPMC) MMC, follow these steps:

1. Click **Start > Run**, type **MMC**, and click **OK**. (You can use **Start > Start Search > MMC >** and click Enter.)
2. From the menu, select **File > Add / Remove Snap-in**.
3. Select **Group Policy Management snap-in** and click **Add**.
4. Click **OK**.
5. From the menu, select **File > Save As**.
6. Type the name **GPMC.msc** and save the MMC either on the desktop or in Administrative Tools.

To create a new GPO in the GPMC tool, follow these steps:

1. Expand Forest, Domains, and your domain name.
2. Right-click the folder **Group Policy Objects** and select **New**.
3. Give your new GPO a descriptive name so that you know what is configured in the GPO.

To edit the new GPO, right-click the new GPO in the **Group Policy Objects** folder and select **Edit**. This opens the GPO in the Group Policy Object Editor (GPOE).

To link a GPO to a site, domain, or OU in the GPMC tool, follow these steps:

1. Expand the appropriate folder to be able to view the target container.
2. Click the desired GPO and drag it to the target container and release. This creates a link between the GPO and the container.

EXAM ALERT

The exam focuses on processing order, blocking inheritance (enforced), delegation, loopback processing modes, and so on.

CAUTION

Use Care When Dealing with GPOs Two GPOs are provided by default in every new domain. They are the Default Domain Policy and the Default Domain Controllers Policy. These policies are generally LEFT ALONE, with no new settings added. These policies have many carefully conceived, preconfigured settings to control and secure your domain and domain controllers (DCs).

You might make an occasional adjustment to a preconfigured setting or two inside these policies, but these changes should be carefully considered, planned, formally approved by senior IT administration, and carefully implemented. If you want to add GPO settings to the domain or to the DCs, create new GPOs with your desired settings and link them in the proper locations.

Group Policy Settings

Now that you know how GPOs are processed, what can you do with them anyway? The GPO that was used on Windows Server 2003 and Windows XP had about 1,700 settings (1,671, as of March 31, 2005). The new GPO for Windows Vista has approximately 2,500 settings (2,495 with the initial release of Vista, to be exact). So what can you do with a GPO in Windows Vista? A lot and then some. The truth is that every configurable parameter of the operating system and every configurable parameter of every application that uses the Registry can be controlled with a GPO. Even if the Registry key or value doesn't exist, it can be added by GPO and then configured by GPO. So the real answer is that approximately everything on the computer that uses or could use the Registry can be controlled by GPO.

The next intelligent question might be "So what are they going to test me on?" That is an excellent question. You're going to look at a handful of specific GPO uses and settings that are potential targets on the exam.

CAUTION

GPOs Are Powerful Mojo GPOs can cause you significant trouble if you create and link them in the wrong places. If you are following along with the book on these settings, banging around inside GPOs, toggling on and off settings, and so on, it is a good idea to create yourself a new, empty OU to link your new trial GPOs to. I usually call my bogus OUs *BOGUS*. Then you can create user objects and computer objects, place them inside the BOGUS OU, link your new GPOs to the BOGUS OU, and then test the GPOs. Use extreme caution if you plan to have the GPO affect the computer that you use regularly. GPOs can and will change a computer's behavior, and sometimes for the worse. You actually need at least one computer to test out the computer settings. Virtual machines perhaps?

Desktop Settings

One of the first target areas has to do with locking down your Desktop settings. Remember that GPOs have two halves: the computer configuration half and the user configuration half. Desktop settings are user-based settings, so you can find these settings in a GPO under User Configuration > Administrative Templates > Desktop, as shown in Figure 3.8.

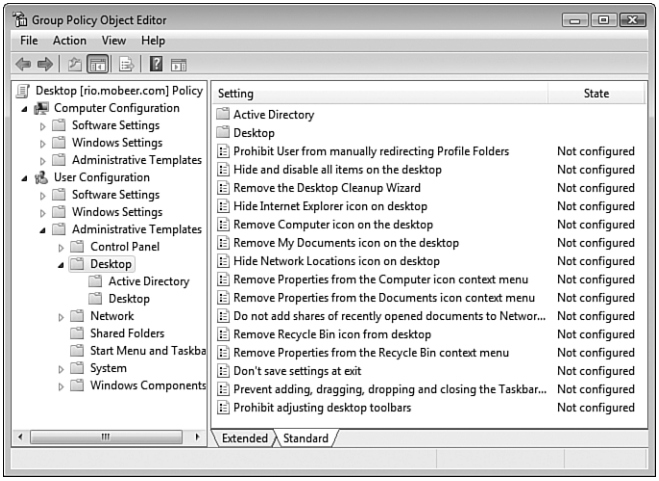

FIGURE 3.8 Desktop controls by GPO are in the user configuration half.

Software Deployment by GPO

The next area to look at is software deployment GPOs. These are used to deploy applications to many computers or users automatically, over the network.

Software can only be *assigned* to the computer by GPO. Software can also be *published* or *assigned* to the user by GPO. The exam question should identify if the target is the computer or the user. Read the exam question carefully.

EXAM ALERT

If a software deployment package is assigned to either the computer or user, it is mandatory and is not optional. The software is deployed at computer bootup or at user logon (unless a slow link is detected).

If the software deployment package is published to the user, it is optional and you may, at your discretion, choose to install the software or choose not install the software (again, unless a slow link is detected).

If the software is assigned to the computer, it is installed at computer bootup, by default. If the software is assigned to the user, it is installed at user logon, by default. If the software is published to you (the user), you have to install the application by using Control Panel > Programs > Get Programs.

Applications can also be configured for deployment by enabling the Auto-install This Application By File Extension Activation setting. This means that if the

application being published is Excel, for example, you might trigger its installation by double-clicking on a file with an `.xls` extension.

GPOs can be used to deploy application software packages with the following extensions:

- `.MSI`—A Microsoft Installer package. This is the preferred software deployment package format. These files can be installed automatically, uninstalled automatically, and even repair themselves (application maintenance) if any of the application's files on the client computer go missing or corrupt.
- `.MST`—A Microsoft Transform file. These files are used to modify the installation behavior of an `.MSI` package—for example, to deploy only Word and Excel from the MS Office suite.
- `.MSP`—A Microsoft Patch file. These files are used to deploy patches for Microsoft and third-party applications. (MS application patches are usually deployed through Microsoft Update these days.)
- `.ZAP`—A script file used to deploy software packages that do not have an `.MSI` file for deployment. This script must be created by an administrator to deploy software when all that is available is a `Setup.exe`, or the like. Although these files can be used to deploy software, the `.ZAP` file cannot be used to maintain or automatically uninstall the deployed software.

The software deployment package must reside on a network share, and users must have at least Allow—Read permissions on the share and on the NTFS permissions for the package. This network share point is called the Software Distribution Point (SDP).

NOTE

Software Distribution Point Permissions Typically, domain administrators are granted Full Control permissions to the SDP and content so they can do whatever they might need to do to maintain and fix any issues that might occur with the software deployment packages.

EXAM ALERT

Remember that only the `.MSI` software deployment packages can be used to automatically uninstall deployed software. You can configure the deployment package to uninstall at next bootup (computer) or Logon (user), or you can configure the GPO to uninstall this application when it falls out of the scope of management. This setting uninstalls the software automatically if the user or computer gets moved from the container (S-D-OU) that the software deployment GPO is linked to, or if the GPO is removed from the container that holds the user or computer. This GPO configuration setting is shown in Figure 3.9.

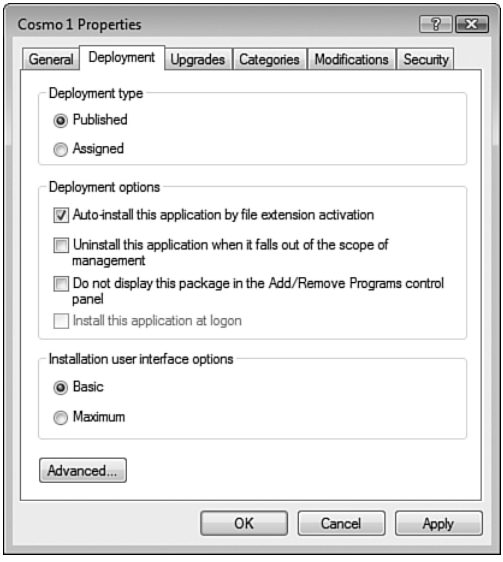

FIGURE 3.9 Enable the software deployment setting to Uninstall This Application When It Falls Out of the Scope of Management.

Software Restrictions

The next major area of GPO category is in Software Restrictions. These GPOs are used to deny all executables except those specifically allowed using the Restricted Default Rule, or used to allow all executables and then disallow specific executables using the Unrestricted Default Rule. These GPO settings are located in the GPO under Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies.

By default, the execution of applications is configured as Unrestricted, as shown in Figure 3.10. Application execution is intended to be controlled by the access permissions (share and NTFS) of the user on the executable.

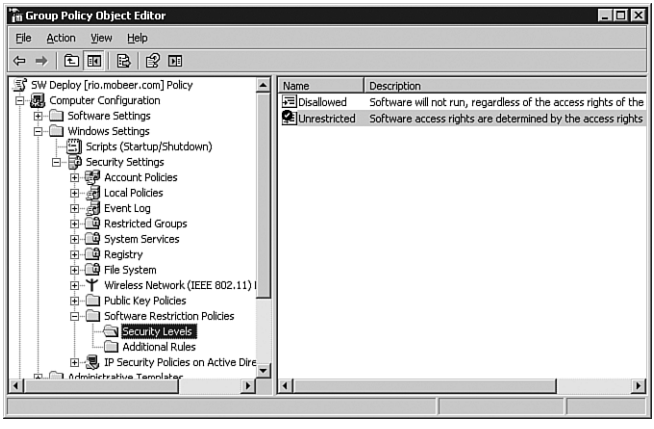

FIGURE 3.10 By default, software execution is unrestricted.

You can configure permissions to keep users from executing applications. You need to do this on each computer where the application resides, a huge task in a large environment. Or you can do it much more easily and on a larger scale by creating a GPO with Software Restriction Rules and then link them appropriately.

Four types of Software Restriction Policy Rules can be used to modify the Default Rule:

- **Certificate Rule**—A digital signature embedded within the executable file.
- **Hash Rule**—A numeric fingerprint of the executable file.
- **Internet Zone Rule**—From tab. They include Internet, Local Intranet, Trusted Sites, and Restricted Sites.
- **Path Rule**—The local path or UNC path to the executable file.

These rules are shown in Figure 3.11.

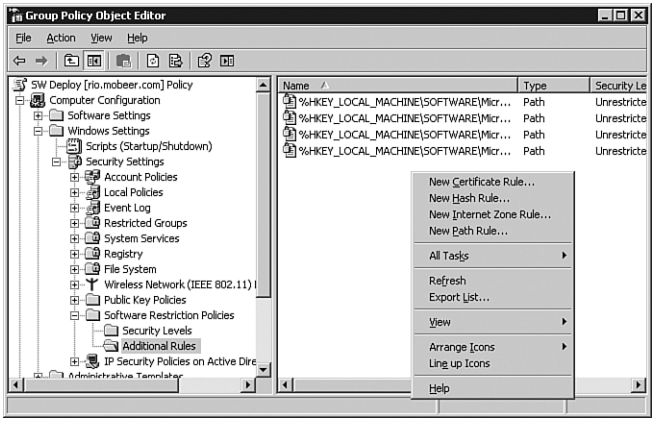

FIGURE 3.11 Modifying the Software Restriction Policy Rules.

These rules often get applied in combinations, and it can get tricky to figure out which GPOs will effectively restrict which applications. As GPOs get processed on the computer, the Software Restriction GPOs are evaluated and then are prioritized in the following order:

1. Certificate Rule—Strongest
2. Hash Rule
3. Path Rule
4. Internet Zone Rule
5. Default Rule—Weakest

EXAM ALERT

If an application fails to run due to Software Restrictions, you might need to add a new Unrestricted Rule of higher priority. An example would be that your OU is configured with a Default Rule set to Restricted. For any application to run, you must configure an Unrestricted Rule of higher priority, such as a Path Rule, as shown in Figure 3.12.

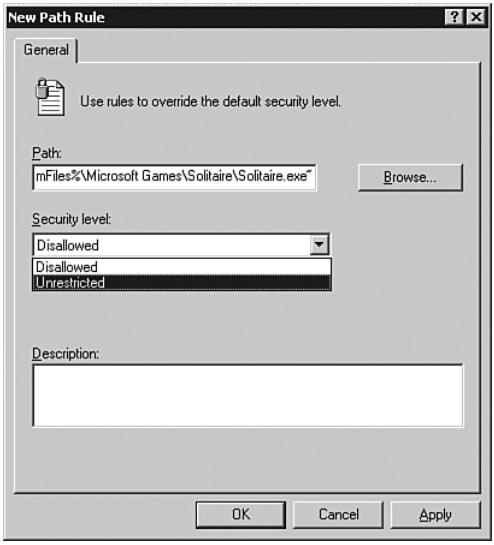

FIGURE 3.12 Setting the Unrestricted Path Rule.

EXAM ALERT

With Path Rules, you may use wildcards within the path statement itself.

The more specific the path, the higher priority it receives when there is a conflict between Path Rules. You can use a single question mark to represent a wildcard for a single character, one question mark per character, or you can use an asterisk as a wildcard to represent any number of characters in the path statement.

For example, the use of `\\Server??` in a Path Rule would satisfy all servers named `\\Server00` through `\\Server99`, as well as `\\Serveraa` through `\\ServerZZ`. The use of the asterisk as a wildcard in a Path Rule might look like `*.vbs`, to allow or restrict all VBS scripts wherever they may be located.

Managing Device Installation

Another powerful control within a GPO that you have over users is the management device installations. This has been a security concern for years. How do you keep users from using USB thumb drives and USB CD/DVD burners to take copies of confidential data and programs away from the office? I have heard

of companies actually gluing the USB mouse and keyboard into the USB ports and then filling all other USB ports with glue just to prevent the use of USB thumb drives that could be used to steal confidential data. Not exactly the perfect solution, but one that addresses the security vulnerability. But now what do you do if the mouse or keyboard fails?

Windows Vista and Windows Server 2008 have addressed and solved this problem through new GPO settings that can control what types of devices can be installed by users, by administrators, or both. These Device Installation GPO settings can be configured on a Windows Vista or Windows Server 2008 computer under Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions, as shown in Figure 3.13.

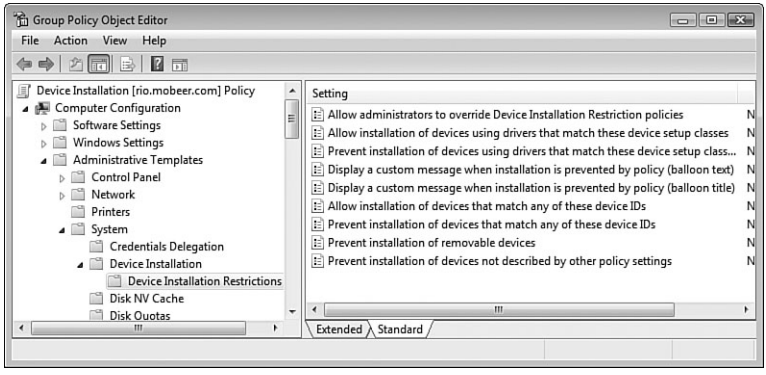

FIGURE 3.13 Setting the Device Installation Restriction policies.

Standard users are not allowed to install many devices. However, by default, they can install a handful of devices, like USB thumb drives.

Devices are identified by Setup Classes (a Registry key) or by Device IDs (a more descriptive label for the devices). By using these identification values, you can configure Prevent Installation policies to include USB thumb drives and other types of devices, as shown in Figure 3.14.

You can configure a GPO to establish a default Prevent Installation of Devices Not Described by Other Policy Settings policy, and then you can configure Allow Installation policies only for specific devices that you want users to be able to install.

The Prevent Installation of Devices Not Described by Other Policy Settings policy setting disallows even an administrator from installing restricted devices. If you need to allow administrators to install restricted devices, you must enable the Allow Administrators to Override Device Installation Restriction Policies, as shown in Figure 3.15, and link it to the appropriate AD container (site, domain, or OU).

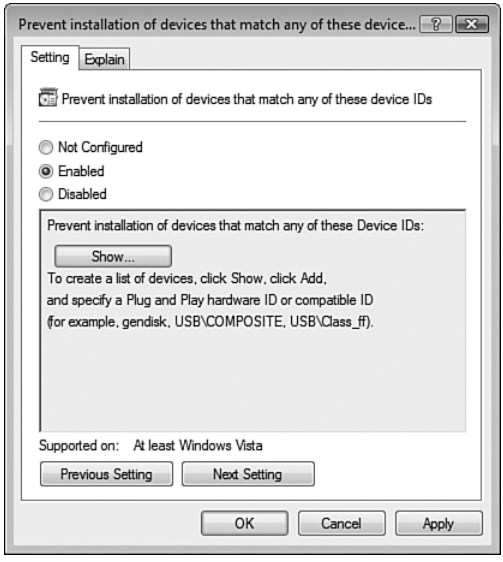

FIGURE 3.14 Preventing installation of devices that match any of these Device IDs.

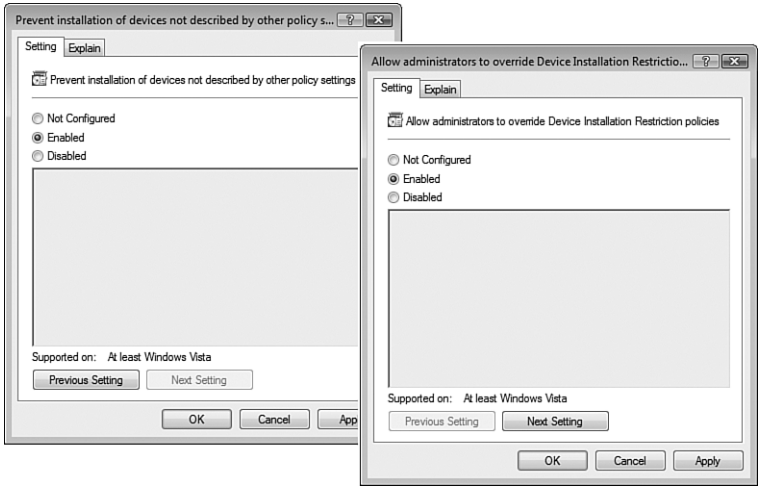

FIGURE 3.15 Setting Allow Device Installation policies for users and for administrators.

The Audit Policy

Auditing is a critical component of the security program for every company. You can configure systems to record what your users do (Success) and what your users attempt to do (Failure). Audit policies are defined within the Local Computer Policy (LCP) and within GPOs. The audit policy is located under Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy. You can configure nine audit policies, as shown in Figure 3.16.

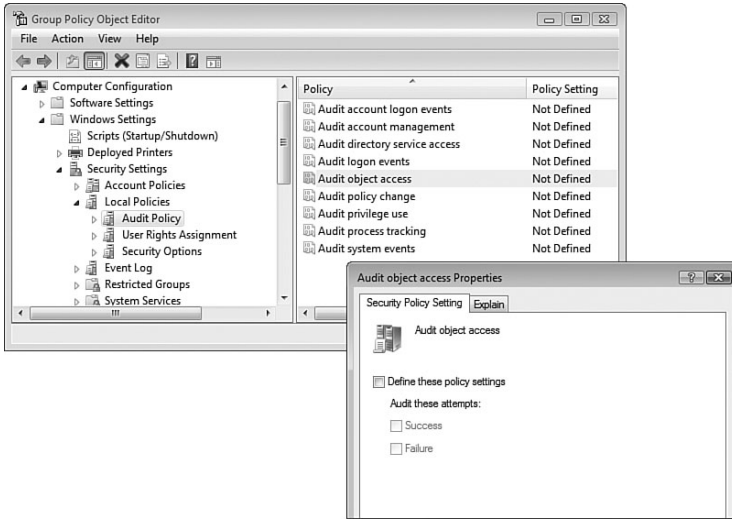

FIGURE 3.16 Configuring the Object Access audit policy within a GPO.

Audited events get recorded in the Security log on the computer where the event occurs and can be reviewed in the Event Viewer on that computer. The Security logs (and any other types of events) from multiple Windows Vista computers can be forwarded to an Event Collector server, a topic addressed later in this chapter.

Most of the audit policies require only the LCP or GPO settings configured to be effective. Two of the audit policies require some additional configuration in addition to the GPO audit policy settings to be effective. They are Directory Service Access and Object Access policies. The additional settings that are required reside on the properties of the objects being tracked by the audit policy and must be configured on the objects' System Access Control List (SACL). (This may also be called the Security Access Control List—SACL.) The GPO turns on the auditing engine, and the SACL identifies specifically which users and which objects will be tracked.

You can access the SACL by following these steps:

1. Right-click on the **Files**, **Folders**, **Printers**, or **AD** objects of interest and select Properties.
2. Select the **Security** tab and click **Advanced**.
3. Select the **Auditing** tab to access the SACL for these types of objects.

TIP

If the Security tab is not visible on AD objects, you must select **View > Advanced Features** from the menu to enable it.

On Registry objects, after enabling the Audit Object Access audit policy, right-click the desired Registry object and select **Permissions**. Click **Advanced** and select the **Auditing** tab. This is the SACL for Registry Keys, Values, and Data, as shown in Figure 3.17.

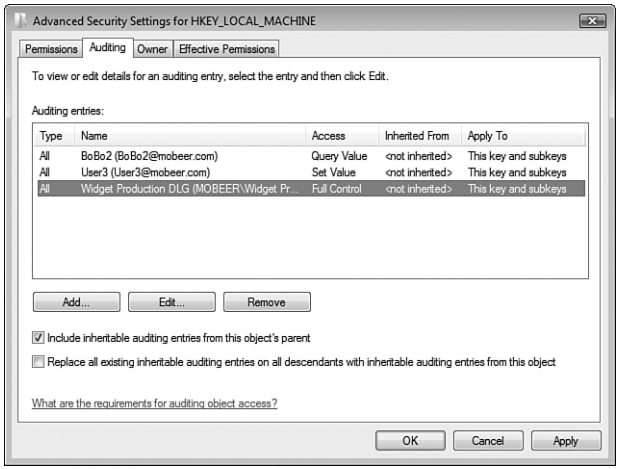

FIGURE 3.17 Configuring the System Access Control List (SACL) in the Registry.

EXAM ALERT

The following is a review of what each audit policy setting accomplishes:

- **Audit Account Logon Events—Logs a user's domain account logons on the domain controller (DC).**
- **Audit Account Management—Logs changes to user objects in AD.**
- **Audit Directory Service Access—Logs access to objects in AD. This audit policy setting requires the additional SACL configuration on the AD objects of interest.**
- **Audit Logon Events—Logs a user's local account logons on the local computer.**
- **Audit Object Access—Logs access to Files, Folders, Printers, and Registry components (Keys, Values, and Data). This audit policy setting requires the additional SACL configuration on the objects of interest.**
- **Audit Policy Change—Logs changes to user rights, auditing, or trust settings within GPOs.**
- **Audit Privilege Use—Logs the use of rights that have been granted.**
- **Audit Process Tracking—Logs actions of and interactions between applications.**
- **Audit System Events—Logs shutdowns and events that affect the System or Security logs.**

Understand the difference between the Audit Account Logon Events and the Audit Logon Events audit policies!

Point and Print Restrictions

Point and Print restrictions allow you to control access to selected shared printers on the corporate network. By default, printers are shared with the permissions set to Allow—Print for the Everyone group. This says that any user can connect to a shared printer, automatically download any required printer drivers, and submit print jobs to that device. Permissions can be adjusted on the printer properties to further control this access. The Point and Print restrictions in a GPO can be used in addition to these permissions to control printer access for large groups of users in an AD environment.

This setting is located under User Configuration > Administrative Templates > Control Panel > Printers, as shown in Figure 3.18.

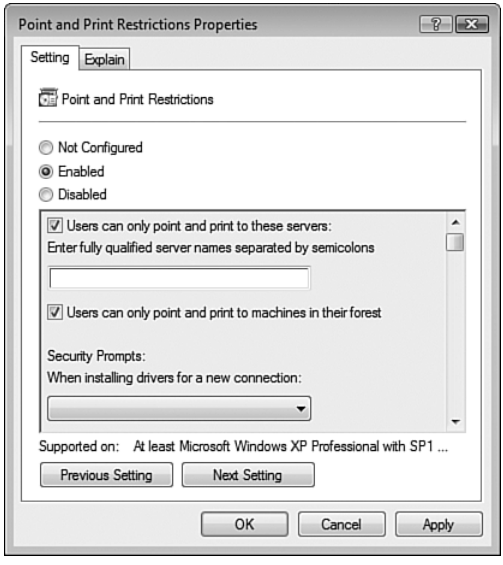

FIGURE 3.18 Configuring Point and Print restrictions.

The fully qualified domain name (FQDN) of the print server must be added to complete the GPO setting.

This GPO setting requires that you construct a list of print servers that the users are allowed to download drivers from and then submit print jobs to. You can further restrict the driver download to only those drivers that have been tested, approved, and digitally signed by Microsoft's Windows Hardware Quality Labs (WHQL), the testing arm of Microsoft for third-party drivers.

Digital Certificates and Authenticode

As users connect to web servers, their browsers download the HTML file and image files and also download and execute active content, like ActiveX controls. Active content, also called *mobile code*, is a major source of malware (viruses and spyware) and is often heavily restricted in a corporate environment.

To ensure that your ActiveX controls are safe and usable by all who visit your website is to have the ActiveX control tested and digitally signed by Microsoft. When an ActiveX control is signed by Microsoft, it is called *Authenticode*, and it is generally trusted to be safe for your users to run. However, on occasion, these tested and approved ActiveX controls can still conflict with other software running on your client computers, so having it signed by Microsoft is still not a guarantee of safety.

CAUTION

Be Careful with Authenticode Restrictions Enabling restrictions on your browsers to allow only approved publishers of Authenticode enhances the security of browsing but can cause web applications and other website functions that rely on unsigned and unapproved publishers of ActiveX controls to fail.

You can restrict the browsers on your users' computers to execute Authenticode only from a select list of publishers that you approve. To do this, you must enable a setting in a GPO that is located under User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Authenticode Settings. The setting is labeled Enable Trusted Publisher Lockdown. This setting, shown in Figure 3.19, disables users from accepting any certificates (used in the Authenticode) from publishers that aren't on your approved publishers list.

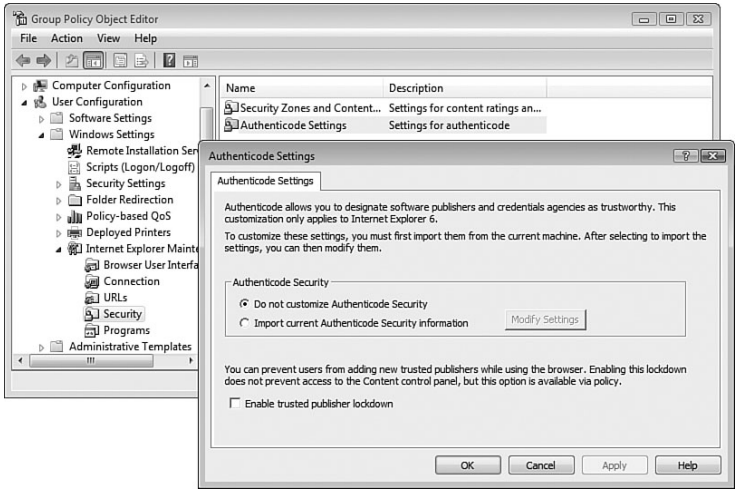

FIGURE 3.19 Configuring trusted publisher lockdown.

Troubleshooting Policy Settings

With all the complexity of GPO processing through the series of L-S-D-OU-OU-OU, and with Block Inheritance and Enforced settings, you might easily recognize that, on occasion, what you get from your collection of GPOs isn't exactly what you expected. To help you sort through this maze of policies and settings, Microsoft has provided several different tools.

Group Policy Results and Group Policy Modeling

The first two tools, and probably the most recommended, can be accessed within the Group Policy Management Console (GPMC):

- Group Policy Results
- Group Policy Modeling

These two tools and a summary from the Group Policy Results tool, are shown in Figure 3.20.

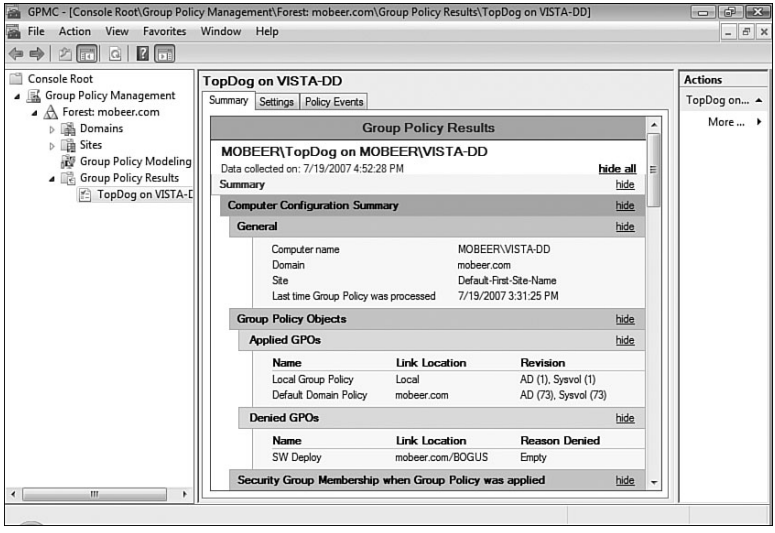

FIGURE 3.20 Using the Group Policy Results tool in the GPMC.

The Group Policy Results Tool

The Group Policy Results tool allows you to identify the effective GPOs and their settings that configure and control the user's session on the computer. You specify which computer and which user to run the analysis on. The Group Policy Results tool performs its analysis based on where the specified computer account actually is located within AD and where a specified user account actually is located within AD to produce the effective GPO results. The Group Policy Results tool is often called the "What is" analysis tool.

The Group Policy Modeling Tool

The Group Policy Modeling tool is used to experiment with "What if" scenarios. It allows you to specify a computer account and a user account to analyze. It then allows you to manipulate where the computer account might be placed within AD and where the user account might be placed within AD. Finally, the Group Policy Modeling tool calculates the effective GPOs and their settings that configure and control the user's session on the computer, based on their newly proposed positions within AD.

Resultant Set of Policies (RSoP)

Another tool that is available in Windows Vista was available in earlier operating systems. It is called the Resultant Set of Policies (RSoP) tool. This tool is still available in Windows Vista as a snap-in to the Microsoft Management Console (MMC) and must be assembled to be accessed.

Just like the Group Policy Results tool, you select which computer and which user to run the analysis on. The RSoP tool performs its analysis based on where the specified computer account actually is located within AD and where a specified user account actually is located within AD to produce the results. The Resultant Set of Policy tool is also called a "What is" analysis tool because it too is based on the objects' actual locations in AD.

As shown in Figure 3.21, the RSoP tool presents the results like a GPO is formatted. This makes a quick overview more difficult than the summary of settings that is presented with the newer Group Policy Modeling and Group Policy Results tools inside the GPMC, and explains why this might not be your first choice of GPO analysis tools.

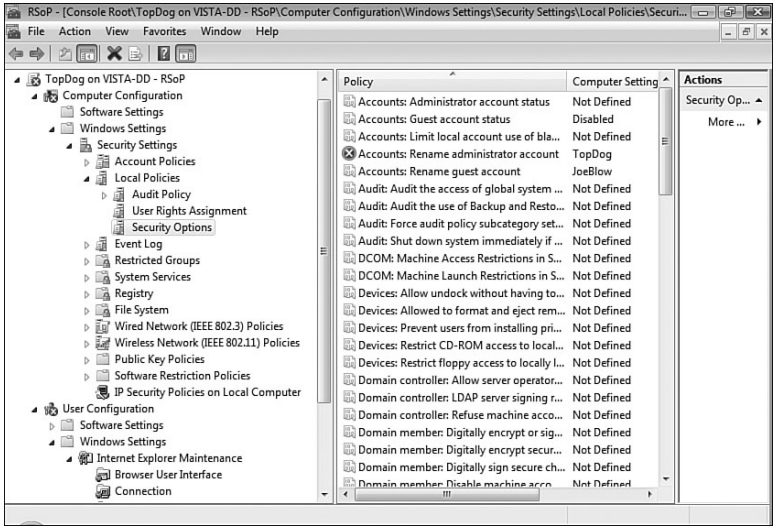

FIGURE 3.21 Using the Group Policy Results tool in the GPMC.

The X icon in Figure 3.21 identifies that a security identifier (SID) failed to resolve to a name. This is usually the result of a renamed or deleted user or computer account.

EXAM ALERT

This RSoP tool is not the recommended tool to use for GPO analysis and troubleshooting but is still available to analyze the effective policies for a computer and user session based on their actual positions within AD.

`GPResult.exe` Command-Line Tool

A third tool to perform a similar analysis is the command-line tool called `GPResult.exe`. This tool analyzes only the local machine where the command is executed and the user who is currently logged on to that machine. The output is ASCII text. It identifies the computer and its configuration and status on the network and also its position in AD. Then `GPResult` reports on all the GPOs that affect the computer. `GPResult` then repeats the process for the user who is logged on to the computer.

Scheduling Tasks

Often, the best time to perform maintenance for performance and disaster recovery is late, late at night, when all the users are at home and asleep, and the servers and the network are at their quietest. The problem is that at that time of the night, all the administrators are also at home and fast asleep. So how should you get your maintenance tasks running at two o'clock in the morning? Why, the Task Scheduler is your tool to do this, of course.

The Task Scheduler is located in Control Panel > System and Maintenance > Administrative Tools. It has a new look and feel in Windows Vista, and has features and capabilities like never before.

The old Task Scheduler in Windows XP and even in Windows Server 2003 was (is) pretty basic; to use it, you followed these steps:

1. Select an executable or script to run.
2. Input credentials to run the task.
3. Set the schedule.

You were done in about three steps.

TIP

The Task Scheduler relies on an underlying service named (Surprise!) the Task Scheduler service. This service may have been stopped for security and performance reasons. If you plan to configure scheduled tasks, you should verify that the Task Scheduler service is started.

The new Task Scheduler has a large library of preconfigured, system-related tasks. Some tasks are active and are already performing their duties in the background. Some tasks are lying dormant, waiting for someone to set a valid trigger to activate them.

As shown in Figure 3.22, the library of preconfigured tasks covers a wide range of targets.

To make adjustments to the existing tasks, click the **Properties** hyperlink in the Actions pane on the right. This brings up the configuration details, as shown in Figure 3.23. The General tab shows which credentials are used to run the task.

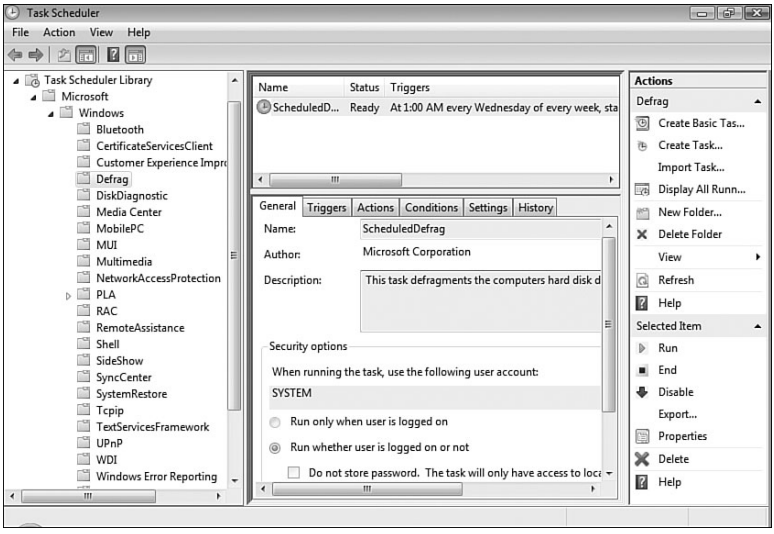

FIGURE 3.22 Preconfigured Windows tasks are available in the Task Scheduler.

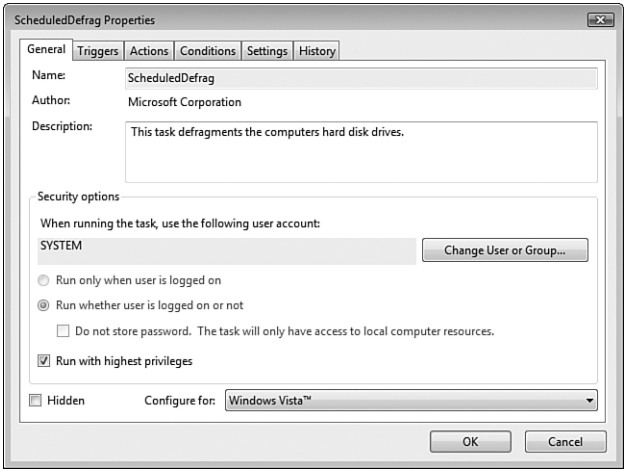

FIGURE 3.23 The properties of a scheduled task.

EXAM ALERT

On the Triggers tab, you can configure what causes your application to run. As you can see in Figure 3.24, you have many new options to choose from. Notice that triggers can even be generated from specified events within Event Viewer. Multiple different triggers can be included on the Triggers list.

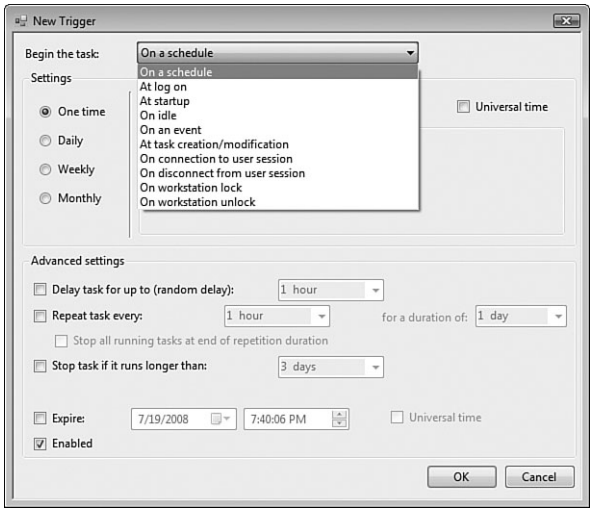

FIGURE 3.24 The triggers that launch a scheduled task now include At Log On and At Startup.

EXAM ALERT

On the Actions tab, you can configure what the Trigger event causes to happen. As you can see in Figure 3.25, you can start a program, send an email, or display a message on the console. Multiple actions can be included on the Actions list.

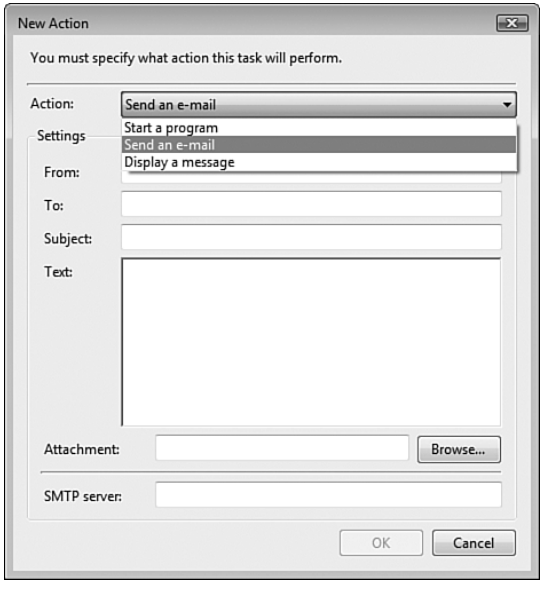

FIGURE 3.25 Actions now include Start a Program, Send an E-mail, or Display a Message on the Console.

A new setting on the Conditions tab is to start the task only if a specified network connection is available. The Settings tab has a new option on what to do if an instance of the task is already running. The choices include

- Do Not Start a New Instance
- Run a New Instance in Parallel
- Queue a New Instance
- Stop the Existing Instance

And finally, the History tab shows a log of activity related to this one task.

Tasks are now recorded in XML files. These XML files can be easily exported and imported onto other Windows Vista computers.

Command-Line Task Scheduler Tools

Surprisingly, the old `AT` command-line Task Scheduler tool is still around and kicking. But the recommended command-line tool to use is called `SchTasks.exe`. This tool isn't new in Vista but is newer than `AT`.

While `SchTasks` can't use triggers other than the clock, and can launch only executables and scripts, you can use `SchTasks` with these switches to perform the following functions regarding scheduled tasks:

- **Run**—Launches the scheduled task immediately
- **End**—Stops the currently running scheduled task
- **Query**—Displays all scheduled tasks
- **Change**—Changes the properties of the scheduled task
- **Create**—Creates a new scheduled task
- **Delete**—Deletes the scheduled task(s)

You should be familiar with these basic functions available with this command-line utility for the exam.

Event Viewer and Event Forwarding

Event Viewer is a tool used to monitor the health of the computer. Event Viewer has had a significant overhaul in Windows Vista and is now closely integrated with Task Scheduler and the Reliability and Performance Monitor. You can access Event Viewer in Administrative Tools and use it to perform the following functions:

- View and filter events from a multitude of preconfigured logs.
- Create and save custom event filters and views.
- Configure tasks to run in response to specified events.
- Configure and manage *event subscriptions*.

The preconfigured logs fall into two categories—Windows Logs and Applications and Services Logs—as shown in Figure 3.26.

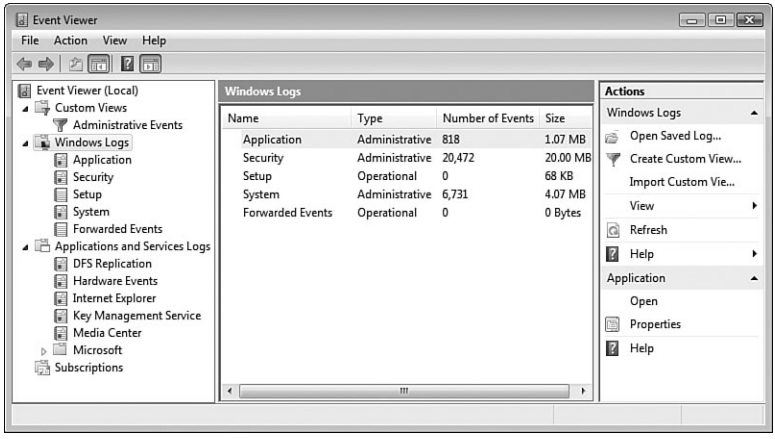

FIGURE 3.26 The main window in Event Viewer shows the Windows Logs and Applications and Services Logs.

As you expand Applications and Services Logs > Microsoft > Windows, you discover dozens of additional, preconfigured event logs. These logs address specific services and features of the operating system and can be used to identify problems, before they start, as well as provide diagnostic and troubleshooting information after something unexpected has happened.

There are two more collections of logs available within Event Viewer:

- **Analytic Logs**—Describe program operations and indicate problems that cannot be addressed with human intervention. Analytic logs generate a high volume of output.
- **Debug Logs**—Used to help developers troubleshoot issues with their programs.

EXAM ALERT

These two logs are hidden by default due to their specialized nature and large volume of output. You can make them visible and functional by enabling them from the View > Show Analytic and Debug Logs menu item, as shown in Figure 3.27.

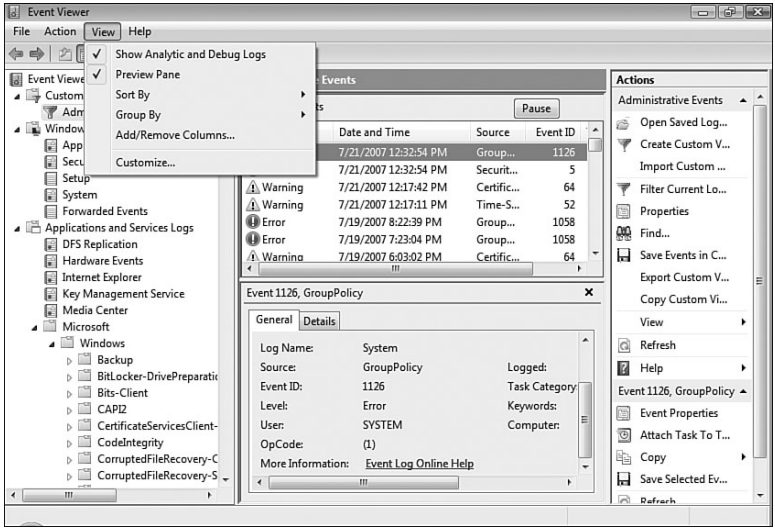

FIGURE 3.27 Showing the Analytic and Debug Logs in Event Viewer.

Event Forwarding

Event Forwarding is used to consolidate events from multiple computers, called *Source computers*, onto a single monitoring station, called the *Collector computer*. Event types include all the event categories in the Windows Logs and Applications and Services Logs. Both Source and Collector computers must be specially configured for Event Forwarding to be successful.

TIP

To configure Event Forwarding, you should log on to the Source and Collector computers using a domain administrator user account.

Source Computer Configuration

On the Source computers, you must configure the Windows Remote Management utility by executing the following command at an elevated privilege command prompt:

```
winrm quickconfig
```

This command makes some changes to your system, including setting the WinRM service to auto start; creates a WinRM Listener on HTTP to accept Web Services for Management (WS-Man) requests—a mini, nonuser-configurable web server); and opens the firewall for WinRM services.

You must also add the computer account of the Collector computer to the local Administrators group on each Source computer.

NOTE

Finding Computers You must enable the adding of computer accounts to the local Administrators group on each Source computer by selecting **Object Type > Computers** in the Select Users, Computers or Groups dialog box in the local Administrators group properties.

Collector Computer Configuration

On the Collector computer, you must configure the *Windows Event Collector Utility* by executing the following command at an elevated privilege command prompt:

```
wecutil qc
```

This command initializes the Windows Event Collector on the Collector computer. Now you are ready to create subscriptions on the Collector computer to Source computer events.

NOTE

Required Services The *Windows Remote Management (WinRM) service* and the Windows Event Collector Service must be started on the Source and Collector computers. By default, these services are set to start up manually. You should configure them for automatic startup to ensure proper functionality and future use of their services.

EXAM ALERT

Here's a quick review:

- **You must configure the Windows Remote Management utility by running `winrm` on the Source computers.**
- **You must configure the Windows Event Collector Utility by running `wecutil` on the Collector computer.**
- **You should familiarize yourself with the basic functions of these two commands by running the executables followed by the `/?` switch.**

To configure subscriptions, in Event Viewer on the Collector computer, right-click **Subscriptions** in the left pane and select **Create Subscription**. The Subscriptions Properties page is shown in Figure 3.28.

NOTE

First Things First Subscriptions can be established only with properly configured Source computers.

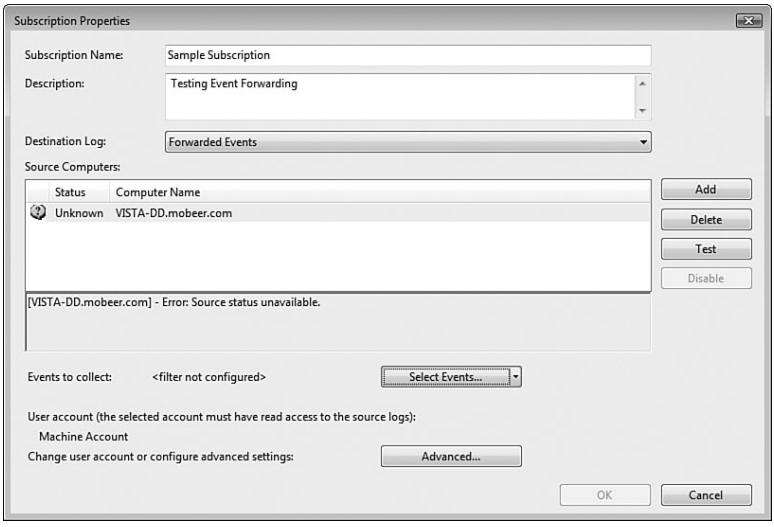

FIGURE 3.28 Configuring an event subscription on the Collector computer.

By clicking **Select Events**, you see that events can be largely unfiltered to acquire large amounts of data or finely filtered to acquire only a very specific and smaller number of events. The Query Filter dialog box for the Subscription is shown in Figure 3.29.

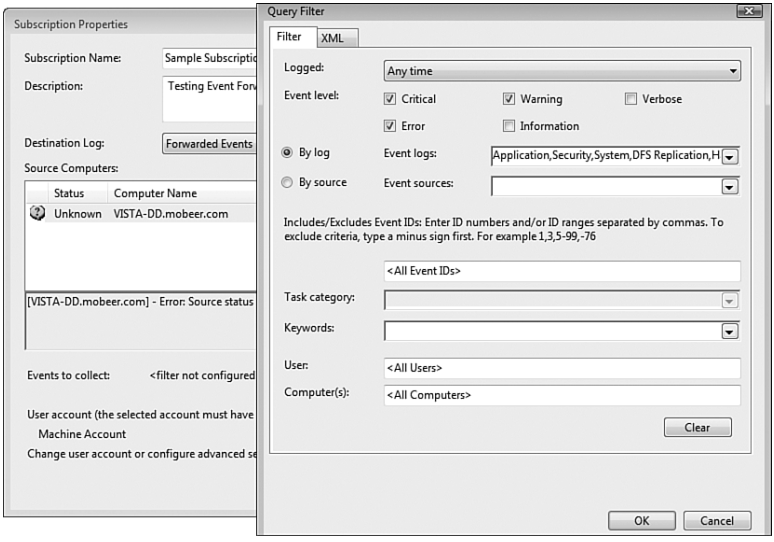

FIGURE 3.29 Configuring a Query Filter to limit the types of events collected on the Collector computer.

The Advanced button on the Subscription Properties dialog box allows for the configuration of the account that will read the log files. This account must have permissions to access the log files and is the typically the computer account that you placed in the local Administrators group on the Source computers. You can also configure the forwarded event delivery for Bandwidth or Latency optimizations.

EXAM ALERT

Also on the Advanced Subscription Settings dialog box, you can configure events to be forwarded using the HTTP protocol over port 80 (the default), or they can be transmitted securely using HTTPS, which is the HTTP protocol over a Secure Sockets Layer (SSL) tunnel. The HTTPS protocol runs over port 443 and requires a computer certificate to authenticate the Source computer to the Collector computer and to establish the encrypted SSL tunnel. Any firewalls between Source computers and the Collector computer require the appropriate port (80 or 443) to be opened. The User Account, Event Delivery Optimization, and transmission Protocol configuration settings are shown in Figure 3.30.

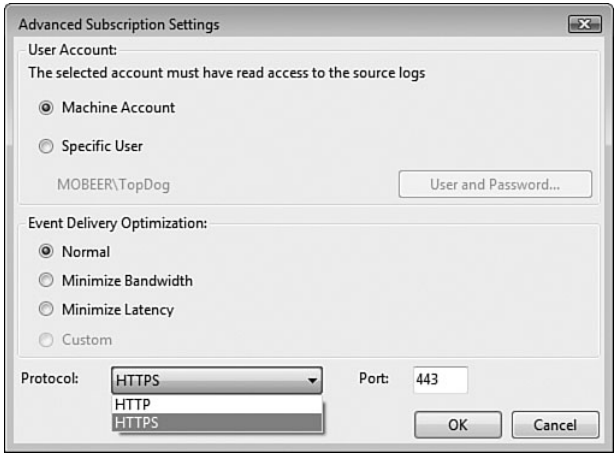

FIGURE 3.30 Advanced Subscription Settings provides access to the User Account, Event Delivery Optimization, and transmission Protocol configuration settings.

Reliability and Performance Monitor

Whereas Event Viewer allows you to monitor system and application events, Reliability and Performance Monitor (RPM) allows you to monitor and log the reliability and performance of your computer. This is the new, upgraded version of the old PerfMon tool that has been around since the NT days.

RPM has three monitoring tools:

- **Resource View**—Provides a quick look at CPU, disk, network, and memory utilization in real time.

- **Performance Monitor**—Uses collections of counters (a *Data Collector Set*) to monitor and log specific resource components in real time or in written logs, for historical review and analysis.
- **Reliability Monitor**—Monitors and logs software, operating system, and hardware failures to present an overview of the system's stability over time.

The RPM tool can be accessed in Administrative Tools. The main dialog box for RPM is shown in Figure 3.31.

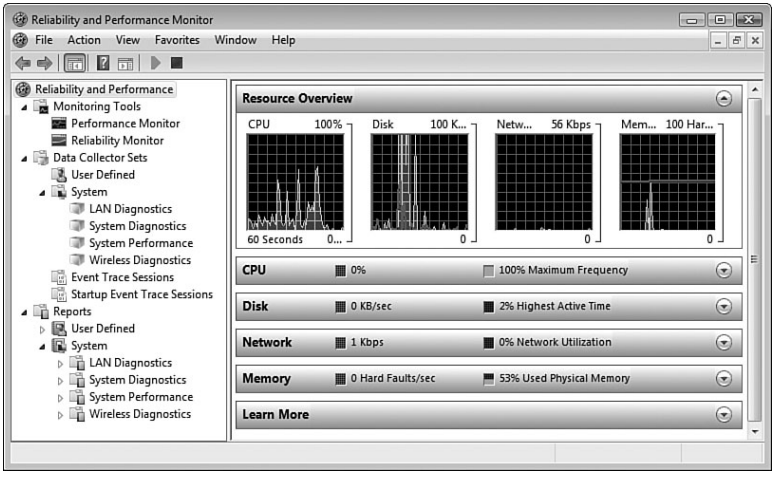

FIGURE 3.31 The Resource Overview is presented when you open the Reliability and Performance Monitor.

Data Collector Sets (DCSs)

The actual data collection and logging is performed by using Data Collector Sets (DCSs).

NOTE

Data Collector Sets Versus Event Forwarding Collector Don't confuse the Data Collector Sets in RPM with the Event Forwarding Collector computer.

EXAM ALERT

There are several preconfigured System Data Collector Sets. They include

- **LAN Diagnostics**
- **System Diagnostics**
- **System Performance**
- **Wireless Diagnostics**

These tools provide a fast and easy way to collect information on the main system functions.

You can also create your own DCSs to log any combination of performance counters available on the system. Additional performance counters may get added to the system over time as you add features and services and install applications on the computer. A sample, custom Data Collector Set is shown in Figure 3.32.

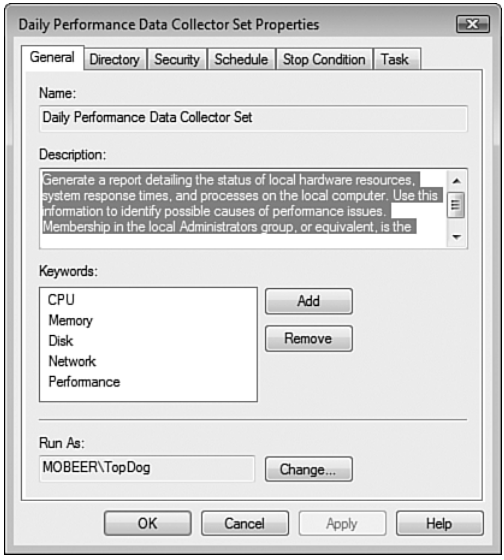

FIGURE 3.32 A custom Data Collector Set.

On the General tab, you can describe the details of your custom DCS and configure the credentials for running the log. On the Directory tab, you can configure where the log files are written to, as well as the format for the naming convention used for the DCS log files. The Security tab is the place where you can configure who can access and modify the DCS parameters. The Schedule tab is the place where you configure the Start conditions for the DCS. The Schedule tab is shown in Figure 3.33. You'll notice that you can schedule the collector to run on a daily basis, and you can add multiple schedules.

FIGURE 3.33 The Schedule tab on a Data Collector Set indicates when the collector begins collecting.

The Stop Condition tab is the place where you configure what terminates the DCS. The stop condition can be an amount of time or some number of megabytes consumed by the log file. This tab is shown in Figure 3.34.

FIGURE 3.34 The Stop Condition tab on a Data Collector Set indicates when the collector stops collecting.

Finally, the Task tab allows you to configure an executable or script to run when the DCS stops. This integrates with the Task Scheduler to perform the launching of the specified task.

EXAM ALERT

The output from RPM can be reviewed in the RPM tool, or it can be exported into a SQL database. This would usually be done when there is a large number of systems being logged with lots of data, and a more detailed analysis is required.

The tool to use to convert the standard log file into one compatible is an executable called `Relog.exe`, included with Windows Vista. This tool allows you to adjust the counters (only for fewer counters, of course), adjust the sampling rate of the logged data (only for larger intervals, of course), and lets you change the file format into binary log files (`.BLG`), comma-separated value log files (`.CSV`), and files compatible with SQL. (`.CSV` files can be imported into spreadsheet applications and databases like SQL or MS Office Access.)

The Performance Monitor

The Performance Monitor, shown in Figure 3.35, is a real-time display of system resources. Using the Performance Monitor, just like a DCS, you configure specific counters to monitor and display. This tool does not record any information. When the data is overwritten by the next pass of the timer mark, the data is lost forever. If you need to keep a record of the data for later review, you must use a Data Collector Set that generates a written log file.

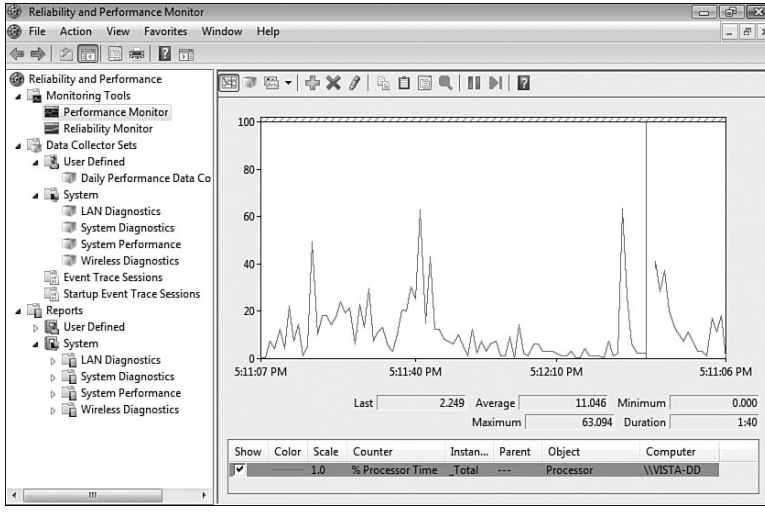

FIGURE 3.35 The Performance Monitor does not record log files. DCSs do record them.

In general, there are four main resource targets for monitoring:

- **RAM**—Monitor Pages Per Second. This value should be less than 20 (average). If it is greater than 20, the system needs more RAM.

- **CPU**—Monitor Percent Processor Time. This value should be less than 70–80% (average). If it is greater than 70%, add a faster CPU, add a second CPU, or move some processes to a less loaded system.
- **Disk Subsystem**—Monitor Percent Disk Time. This value should be less than 50% (average). If it is greater than 50%, add a faster disk, add a faster disk array (RAID 0 or RAID 5), or move some accessed content to a lesser used disk.
- **Network Subsystem**—Monitor Bytes Total per Second. This value should be less than 6MB/s (average). At 6MB/s, the NIC is occupying about 50% of a 100Mbps network. This is too much. If it is greater than 6MB/s, figure out what is sending and/or receiving over the network. You'll probably find that the problem is really that the NIC is failing and should be replaced.

The Reliability Monitor

The Reliability Monitor tracks application, operating system, and hardware failures to present a trend analysis of system stability. The Reliability Monitor is shown in Figure 3.36.

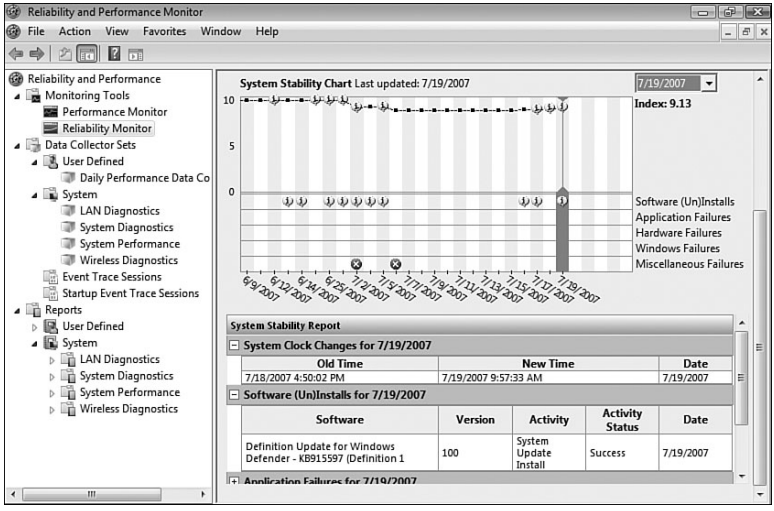

FIGURE 3.36 The Reliability Monitor tracks system failures.

The Index rating in the upper-right corner is an indication of the reliability and stability of the system. You can select any incident on the calendar chart and review details of the incident.

Exam Prep Questions

1. You enable Auditing for Object Access, Success, and Failure in a GPO and link it to the Production OU. After you configure the System Access Control List of the targets of interest, which of the following is NOT logged as a result of this audit policy?

   - ❍ **A.** File access
   - ❍ **B.** Printer access
   - ❍ **C.** Registry changes
   - ❍ **D.** AD object access

2. You have just created a new Group Policy Object. You are considering the proper location to link the GPO to achieve your desired results. Place the following in the proper order that matches how GPOs get processed.

   - ❍ **A.** Site
   - ❍ **B.** Organizational Unit
   - ❍ **C.** Local Computer Policy
   - ❍ **D.** Domain

3. As a security measure, you configure and link a GPO that disallows the installation of USB thumb drives for computers in the Secretary's OU. One of your administrators is implementing a new wireless configuration in the secretaries department. The administrator's automated deployment strategy includes the use of the Wireless Network Setup Wizard. The administrator's deployment fails on 100% of the computers. You need to get the secretaries' computers running on the wireless network. You must not diminish security for the enterprise. What should you do?

   - ❍ **A.** Disable the Computer Configuration half of the Device Installation Restriction GPO.
   - ❍ **B.** Configure a GPO to allow administrators to override Device Installation Restriction policies.
   - ❍ **C.** Disable SSID broadcasts on the wireless access point.
   - ❍ **D.** Implement the MAC address filtering on the wireless access point.

4. You have a domainwide Path Rule configured to disallow the use of an application set to `*\BadApp\badapp.exe`. The application installs in the `C:\Program Files\BadApp\` folder. Users in the R&D OU need to test a system with the

badapp.exe program, and they report that they receive an error whenever they launch badapp.exe. You must allow the use of badapp.exe in the R&D OU and not diminish the security of the company. What should you do? Choose two. Each correct answer presents a complete solution.

- ❍ **A.** Create a Software Restriction policy and link it to the R&D OU. Set the Default Rule to Allow.
- ❍ **B.** Create a Software Restriction policy and link it to the R&D OU. Set the Hash Rule to allow the hash of badapp.exe.
- ❍ **C.** Create a Software Restriction policy and link it to the R&D OU. Set the Path Rule to `Allow *\badapp.exe`.
- ❍ **D.** Create a Software Restriction policy and link it to the R&D OU. Set the Path Rule to `Allow *\Program Files\BadApp\badapp.exe`.

5. Your R&D users access highly confidential data on your HiSec Servers. All R&D users run Windows Vista on their computers. All HiSec Servers run Windows Server 2003 Standard Edition. You are concerned about sniffers on the network and must secure all data transmissions to and from the HiSec Servers. What should you do?

- ❍ **A.** Implement a Secure Server IPSec Policy on the HiSec Servers.
- ❍ **B.** Implement a Secure Server IPSec Policy on the R&D computers.
- ❍ **C.** Implement a Server Request IPSec Policy on the R&D computers.
- ❍ **D.** Implement a Client Respond IPSec Policy on the HiSec Servers.

6. Your company rotates the employees between departments (OUs) regularly for security and cross-training purposes. You have deployed an application to users in your department (OU) by GPO. Because your cost center has paid for the licenses, you need to ensure that this software is not installed on computers used by users outside your OU. What should you do?

- ❍ **A.** Require that all users log off their computers each night so that software deployment GPOs will reapply when they log in each morning.
- ❍ **B.** Disable the Software Deployment GPO setting to install the application by file extension activation.
- ❍ **C.** Implement a Software Restriction Policy with a Default Rule set to Disallowed and a Certificate Rule set to allow the application in your OU.
- ❍ **D.** Configure the Software Deployment package to uninstall the application automatically if it falls out of the scope of the GPO.

7. You convinced one of your vendors to provide you with a personal calendar application that some users might find useful. The regular price of the application is $300 per user, but you got it for $50 per user. You want to make it available to users in your OU that would like to use it. What should you do?

- ❍ **A.** Publish the software package to the computer.
- ❍ **B.** Assign the software package to the user.
- ❍ **C.** Publish the software package to the user.
- ❍ **D.** Assign the software package to the computer.

8. You plan to deploy a software package to computers in your OU. You must configure the permissions required for you to upload the package to the Software Distribution Point (SDP) and for computers to receive the package. You want the security level to remain as high as possible. What should you do? Choose two. Each correct answer presents a partial answer.

- ❍ **A.** Grant the Authenticated Users group the Allow—Read permission.
- ❍ **B.** Grant the Everyone group the Allow—Change permission.
- ❍ **C.** Grant the Administrators group the Allow—Change permission.
- ❍ **D.** Add the computer names to the Trusted Sites list in Internet Explorer.

9. You have two weekly scheduled tasks that are currently running. You need to terminate them both. `GoodApp.exe` needs to run again at its next scheduled time. `OldApp.exe` never needs to run again. What should you do? Choose two. Each correct answer presents a partial solution.

- ❍ **A.** Run the command `SchTasks /end` for the `GoodApp.exe` task.
- ❍ **B.** Run the command `SchTasks /delete` for the `GoodApp.exe` task.
- ❍ **C.** Run the command `SchTasks /end` for the `OldApp.exe` task.
- ❍ **D.** Run the command `SchTasks /delete` for the `OldApp.exe` task.

10. You need to configure Event Forwarding from 10 Windows Vista computers to your Windows Vista computer. What should you do? Choose two. Each correct answer presents a partial answer.

- ❍ **A.** Run the `winrm.exe` utility on your computer.
- ❍ **B.** Run the `winrm.exe` utility on the 10 computers.
- ❍ **C.** Run the `wecutil.exe` utility on your computer.
- ❍ **D.** Run the `wecutil.exe` utility on the 10 computers.

11. You work with nine other administrators in your enterprise. They all seem to create and implement GPOs at their own discretion, without any coordination. You implement a new GPO, and users report that they are not seeing the effect of the new GPO. What three tools could you use to troubleshoot this GPO problem? Choose three. Each correct answer presents a partial answer.

- ❍ **A.** Group Policy Management Console—Group Policy Modeling
- ❍ **B.** Computer Management
- ❍ **C.** `GPUpdate.exe`
- ❍ **D.** Resultant Set of Policies
- ❍ **E.** Active Directory domains and trusts
- ❍ **F.** Local Computer Policy
- ❍ **G.** `GPResult.exe`
- ❍ **H.** Remote Desktop Connection

12. You are preparing a report to management on the performance of several of the computers that you are responsible for in your company. You are deciding the best method of extracting information for analysis in a third-party program. Which of the following are available export formats for the Reliability and Performance Monitor (RPM) tool? Choose two. Each correct answer presents a partial answer.

- ❍ **A.** `*.evt`
- ❍ **B.** `*.csv`
- ❍ **C.** `*.bin`
- ❍ **D.** `*.blg`

13. You have created a scheduled task to run every night at midnight on a server using the credentials of the Administrator account. You check the logs and discover that the task has failed to run any night over the past week. You test the executable and it works just fine. You need the task to run every night. What should you do?

- ❍ **A.** Run the `SchTasks /Run` command-line utility on the server.
- ❍ **B.** Delete and re-create the Scheduled Task using the same parameters.
- ❍ **C.** Configure the task to run using your credentials.
- ❍ **D.** Configure the firewall on the server to allow inbound UDP port 500.

Answers to Exam Prep Questions

1. Answer **D** is correct. AD object access are NOT logged as a result of this audit policy. After the SACL is configured, Auditing Object Access tracks access to Files, Folders, and Printers and also tracks Registry changes. Directory Service access tracks AD object access. Both these audit policies require additional configuration of the SACL on the object(s) of interest.

2. The correct order for GPO processing is **C**, then, **A**, then **D**, and then **B**. L-S-D-OU is the way that policies get processed. The Local Computer Policy is followed by Site policies, followed by Domain policies, and finally followed by OU policies. OU policies process starting with the top-level OU policies, which are then followed by each subsequent child OU's policies walking down the OU hierarchical branch. First, the computer half gets processed, L-S-D-OU, as the computer boots up. Then the user half gets processed, L-S-D-OU, after the user logs in. Together, these establish the desktop and security for the user's session on that computer.

3. Answer **B** is correct. The wireless configuration deployment failed because of the Device Installation Restriction policy. Wireless configuration can be automated on a thumb drive. You can configure the Device Installation Restriction not to apply to Administrators. Disabling the computer half of the GPO would weaken security because it would disable the device installation restrictions. The SSID broadcasts and MAC address filtering both enhance security for the wireless network but would not facilitate the deployment of the wireless configuration to the secretaries' computers.

4. Answers **B** and **D** are correct. The processing priority for the different rules is Certificate Rules override all other rules, followed by Hash, Path, Internet Zone, and finally the Default Rule has the lowest priority and is overridden by any other rules. So to override a Path Rule, you could implement a Hash Rule for the R&D OU, answer B. The most specific Path Rule overrides a less specific Path Rule, so the longer path in answer D would override the shorter Path Rule set at the domain level.

5. Answer **A** is correct. You must implement the Secure Server IPSec policy on the servers. The Secure Server IPSec policy on the Vista clients would require security only for inbound connections. In this case, the Vista computers are the clients and are making outbound connections to the HiSec Servers. The Server Request IPSec policy would allow unsecured connections if a client could not run IPSec. The client respond policy would be required on the Vista computers, not the servers.

6. Answer **D** is correct. The Software Deployment GPO can be configured to uninstall the software when the users are no longer within your OU. Logging off by itself does not cause the software to be removed from computers. File extension activation configures the software package for installation, not removal. Setting the Default Software Restriction Policy to Disallowed would disallow all software from running on your OU. This would not remove any software from computers being used by users outside your OU.

7. Answer **C** is correct. You want to publish the software to the users. This way, only the ones who want to use the application will install it. Software packages cannot be published to computers, only assigned. Even though you got a deal on the software, assigning to the users costs you extra money because all users get the package. Assigning to the computers also costs you extra money, again, because all computers get the software.

8. Answers **A** and **C** are correct. Authenticated users need the Allow—Read permission. Administrators need at least the Allow—Change permission. (Most of the time, administrators grant themselves the Allow—Full Control permission on these SDPs because they may need to make adjustments to the NTFS permissions within the share point. But this is more privilege than is required on the SDP.) Everyone Allow—Change is too much privilege, and adding the computer names to the Trusted Sites list in IE has no benefit in this scenario.

9. Answers **A** and **D** are correct. You simply want to terminate the currently running instance of `GoodApp.exe` but keep the task scheduled for future executions. For this, you use the `/end` switch. You want the currently running instance of `OldApp.exe` to be terminated, and you want `OldApp.exe` to be removed as a scheduled task, so you would use the `/delete` switch on the `SchTasks.exe` command.

10. Answers **B** and **C** are correct. You need to run the Windows Remote Management utility (`winrm.exe`) on the 10 remote Windows Vista computers. These are the Source computers. You want to run the Windows Event Collector utility (`wecutil.exe`) on the Collector computer, your one Windows Vista computer.

11. Answers **A**, **D**, and **G** are correct. The three tools available to analyze how GPOs are being applied are the Group Policy Modeling tool inside GPMC, the older Resultant Set of Policies (RSoP), and `GPResult.exe`. The Computer Management MMC includes several worthy tools, like Local Users and Groups, Disk Management and Services, but it does not analyze GPO processing. GPUpdate reapplies GPOs that have been changed since the last GPO Refresh. Used with the `/Force` switch, it can reapply all GPOs to a user's session, but it does not analyze GPO processing. AD domains and trusts is used to transfer the Domain Naming Operations Master and to assemble and test inter-domain and inter-forest trusts. The Local Computer Policy might be considered one of the policies being analyzed, but it does not analyze GPO processing. Remote Desktop Connection is used to make connections to Terminal Servers, and it does not analyze GPO processing.

12. Answers **B** and **D** are correct. The RPM tool can export into binary log file format (`*.blg`) and the comma-separated value file format (`*.csv`). `*.evt` files are used by Event Viewer as the extension for its log files. `*.bin` files are usually binary files, not binary log files (`*.blg`).

13. Answer **C** is correct. Because the task fails when running with the credentials of the administrator but runs successfully when it is launched using your credentials, use your credentials to launch the Scheduled Task. The `SchTasks /Run` command causes the task to launch immediately. Deleting and re-creating the task with the same parameters does not resolve the credentials issue. UDP port 500 is used by IPSec, which has nothing to do with this issue.

Need to Know More?

The following websites present a wealth of technical information relating to the topics presented in this chapter. When on a web page, you often can find additional hyperlinks that address related topics to help you flesh out your knowledge and understanding of the topic.

NOTE

The Value of TechNet Some of these websites may require a membership to Microsoft TechNet. Microsoft TechNet is one of your most valuable collections of tools and resources available to you as a Microsoft IT Professional. If you don't have one already, and you plan on being professionally responsible for Microsoft computers, you probably need a Microsoft TechNet membership.

1. Windows Vista Step-by-Step Guides for IT Professionals—Many topics:

   http://www.microsoft.com/downloads/details.aspx?FamilyID=311f4be8-9983-4ab0-9685-f1bfec1e7d62&DisplayLang=en

2. Group Policy processing and precedence:

   http://technet2.microsoft.com/windowsserver/en/library/274e614e-f515-4b80-b794-fe09b5c21bad1033.mspx?mfr=true

3. Slow Link detection by XP using ICMP:

   http://support.microsoft.com/kb/816045

4. Group Policy Settings for Windows Vista:

   http://www.microsoft.com/downloads/details.aspx?FamilyID=41dc179b-3328-4350-ade1-c0d9289f09ef&displaylang=en

5. Group Policy Settings for Windows Server 2003 and Windows XP:

   http://www.microsoft.com/downloads/details.aspx?familyid=7821C32F-DA15-438D-8E48-45915CD2BC14&displaylang=en

6. Software deployment by GPO:

   http://technet2.microsoft.com/windowsserver/en/library/bca0be15-7170-4670-a771-753566e3e5781033.mspx?mfr=true

7. Troubleshooting Software deployment GPOs:

   http://technet2.microsoft.com/windowsserver/en/library/655468d7-4462-4b77-81a6-642d9047249a1033.mspx?mfr=true

8. Audit Policy:

   http://technet2.microsoft.com/windowsserver/en/library/e104c96f-e243-41c5-aaea-d046555a079d1033.mspx?mfr=true

9. Software Restriction Policies:

   http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/xpsgch06.mspx

10. Task Scheduler:

    http://technet.microsoft.com/en-us/windowsvista/aa906020.aspx

11. Windows Vista Management Features:

    http://technet.microsoft.com/en-us/windowsvista/aa905069.aspx

    http://technet2.microsoft.com/WindowsVista/en/library/cab7eb3d-7aef-4f43-988b-132f7f9bb5d21033.mspx?mfr=true

12. Event Viewer:

    http://www.microsoft.com/technet/technetmag/issues/2006/11/EventManagement/

13. Event Forwarding over the Internet:

    http://technet2.microsoft.com/WindowsVista/en/library/a84d76d4-d149-4bba-8b8c-750ec797d4b61033.mspx?mfr=true

14. Reliability and Performance Monitor:

    http://technet.microsoft.com/en-us/windowsvista/aa905077.aspx

    http://technet2.microsoft.com/WindowsVista/en/library/ab3b2cfc-b177-43ec-8a4d-0bfac62d88961033.mspx?mfr=true

    http://technet2.microsoft.com/WindowsVista/en/library/1522b01c-69a3-43d2-884a-2af28f74f9b01033.mspx?mfr=true

Index

Symbols

A

B

C

D

E

F

G

H

I

J–K–L

M

N

O

P

Q–R

S

T

U

V

W

X–Y–Z