EXAM CRAM

The Smart Way to Study™

Exam 70-640

MCTS

Windows Server 2008 Active Directory, Configuring

Don Poulton

MCTS 70-640 Exam Cram: Windows Server 2008 Active Directory, Configuring

ISBN-13: 978-0-7897-3791-5
ISBN-10: 0-7897-3791-4

Library of Congress Cataloging-in-Publication Data

Poulton, Don.

MCTS 70-640 exam cram : Windows server 2008 active directory, configuring / Don Poulton. -- 1st ed.

p. cm.

ISBN 978-0-7897-3791-5 (pbk. w/cd)

1. Electronic data processing personnel--Certification. 2. Microsoft software--Examinations--Study guides. 3. Directory services (Computer network technology)--Examinations--Study guides. I. Title.

QA76.3.P667 2008

005.7'1376--dc22

2008034083

Printed in the United States of America

First Printing: September 2008

Associate Publisher
Dave Dusthimer

Executive Editor
Betsy Brown

Development Editor
Deadline Driven Publishing

Managing Editor
Patrick Kanouse

Project Editor
Amanda Gillum

Copy Editor
Gill Editorial Services

Indexer
Tim Wright

Proofreader
Leslie Joseph

Technical Editors
David Camardella
Pawan J. Bhardwaj

Publishing Coordinator
Vanessa Evans

Book Designer
Gary Adair

Composition
Louisa Adair

Introduction

Welcome to *MCTS 70-640 Exam Cram: Windows Server 2008 Active Directory, Configuring*. This book aims to help you get ready to take—and pass—Microsoft Certification Exam 70-640: TS: Windows Server 2008 Active Directory, Configuring. This book contains information to help ensure your success as you pursue this Microsoft exam and the Technology Specialist or IT Professional certification.

This Introduction explains the new generation of Microsoft certifications centering on Windows Server 2008 and how the *Exam Cram* series can help you prepare for Exam 70-640. This chapter discusses the basics of the MCTS and MCITP certifications, including a discussion of test-taking strategies. Chapters 1 through 9 are designed to remind you of everything you need to know to take and pass the exam. The two sample tests at the end of this book should give you a reasonably accurate assessment of your knowledge and, yes, I've provided the answers and their explanations to the tests. Along with the explanations are some particularly useful links to more information on each topic. Each answer also includes a reference to the chapter in the book that covers the topic.

Read this book and understand the material, and you'll stand a very good chance of passing the test. Use the additional links to the other materials and points of reference, and along with actual product use, you will be in excellent shape to do well on the exam.

Exam Cram books help you understand and appreciate the subjects and materials you need to pass Microsoft certification exams. These books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a topic. Instead, they present and dissect the questions and problems that you're likely to encounter on a test. These books work to bring together as much information as possible about Microsoft certification exams.

The MCTS (Microsoft Certified Technology Specialist) certification requires you to have a strong knowledge of the features of Active Directory in Windows Server 2008, in particular the newer features. To move on to the next level, you have to drill down into each feature significantly. The MCITP (Microsoft Certified IT Professional) Windows Server 2008 Administrator and Windows Server 2008 Enterprise Administrator certifications require considerable in-depth information about the particulars of each of the Windows Server 2008 features.

Every Microsoft Windows Server 2008–related certification starts off with Exam 70-640, which this book prepares you for, as well as Exam 70-642, TS: Windows Server 2008 Network Infrastructure, Configuring. From there, if you continue along any of the tracks, each of the IT Pro certifications mandates that you pass one or two other Windows Server 2008–specific exams. Exam 70-646, PRO: Windows Server 2008, Server Administrator, completes the requirements for the MCITP: Windows Server 2008 Administrator certification. The MCITP: Windows Server 2008 Enterprise Administrator certification requires that you pass two additional exams, 70-643, TS: Windows Server 2008 Applications Infrastructure, Configuring, and 70-647, PRO: Windows Server 2008, Enterprise Administrator. Furthermore, the Windows Server 2008 Enterprise Administrator certification requires that you pass one client exam related to Windows Vista, either 70-620, TS: Microsoft Windows Vista, Configuring, or 70-624, TS: Deploying and Maintaining Windows Vista Client and 2007 Microsoft Office System Desktops.

Content included in this book is also covered in the upgrade exams provided by Microsoft for individuals holding the Microsoft Certified Systems Administrator (MCSA) or Microsoft Certified Systems Engineer (MCSE) titles on Windows Server 2003. More specifically, this includes Exam 70-648, TS: Upgrading Your MCSA on Windows Server 2003 to Windows Server 2008, Technology Specialist, and 70-649, TS: Upgrading Your MCSE on Windows Server 2003 to Windows Server 2008, Technology Specialist. Individuals wishing to pass either of these exams will find the content in this book helpful for learning the Active Directory portions of these exams.

The Microsoft Certified Professional (MCP) Program

The MCP Program includes a new generation series of professional certifications as well as a series of traditional program tracks. Each program track boasts its own special acronym. (As a certification candidate, you need to have a high tolerance for alphabet soup of all kinds.)

New Generation Microsoft Certifications

Microsoft has revamped its certification tracks to target individuals' efforts toward the level of detail representing their existing or anticipated employment

needs and capabilities. These tracks are simpler and more specifically targeted than the older certification tracks. In many cases, they can be achieved by passing fewer exams than was the case with the older tracks.

- **MCTS (Microsoft Certified Technology Specialist)**— Typically consisting of one to three exams, these certifications enable you to target your learning program to specific Microsoft technologies. MCTS certifications are available in a broad range of Microsoft technologies, and more will be added as newer technologies become online.
- **MCITP (Microsoft Certified Information Technology Professional)**—By taking one to three additional exams beyond the MCTS level, you can achieve a comprehensive set of IT skills enabling you to be successful at a range of specialized jobs such as design, project management, operations management, and planning. Currently, MCITP certifications are available in the fields of Business Intelligence Developer, Customer Support Technician, Database Administrator, Database Developer, Enterprise Messaging Administrator, Enterprise Project Management with Microsoft Office Project Server 2007, Enterprise Support Technician, Exchange Messaging Administrator, Windows Server 2008 Administrator, and Windows Server 2008 Enterprise Administrator.
- **MCPD (Microsoft Certified Professional Developer)**—Similar to the MCITP certification, this enables you to achieve a comprehensive set of developer-related job skills. Current MCPD certifications are based on .NET Framework 2.0 applications that use Microsoft Visual Studio 2005 and include Web Developer, Windows Developer, and Enterprise Applications Developer. Additional certifications will be released as newer technologies emerge.
- **MCA (Microsoft Certified Architect)**—Enables you to prove a top level of IT business and design skills. Individuals aspiring to this certification must have at least 10 years of advanced IT experience including at least three years of experience as an IT architect. They must also have strong technical and managerial proficiency and follow a rigorous mentoring program that culminates in an oral examination by a panel of certified architects. You can specialize in Messaging or Database or pursue a more general Infrastructure or Solutions program.

Traditional MCP Program Tracks

The traditional program tracks that Microsoft has followed for a number of years certify individuals on technologies up to and including Windows Server 2003:

- **MCSE (Microsoft Certified Systems Engineer)**— Anyone who has a current MCSE is warranted to possess a high level of networking expertise with Microsoft operating systems and products. This credential is designed to prepare individuals to plan, implement, maintain, and support information systems, network, and internetworks built around Microsoft Windows 2000 or Windows Server 2003 and its BackOffice Server family of products.

  The Windows Server 2003 MCSE is the last certification that Microsoft plans to award on this program. Obtaining this credential requires an individual to pass six core exams and one elective exam. The core exams include four networking system exams, one operating system exam, and one design exam. Beginning with Windows Server 2008, the MCSE has been replaced by the MCITP credential already mentioned.

- **MCSA (Microsoft Certified Systems Administrator)**— This certification program is designed for individuals who are systems administrators but have no need for network design skills in their current career path. An MCSA on Windows Server 2003 candidate must pass three core exams plus one elective exam. Beginning with Windows Server 2008, the MCSA has been replaced by the MCTS and MCITP credentials already mentioned.

- **MCP (Microsoft Certified Professional)—**This is the least prestigious of all the certification tracks from Microsoft. Passing one of the major Microsoft exams qualifies an individual for the MCP credential. Individuals can demonstrate proficiency with additional Microsoft products by passing additional certification exams.

- **MCSD (Microsoft Certified Solution Developer)**—The MCSD credential reflects the skills required to create multitier, distributed, and COM-based solutions, in addition to desktop and Internet applications, using new technologies. An MCSD must pass three core exams and one elective exam. The last iteration of the MCSD program validated competency in the 6.0 level of Microsoft Visual C++, Microsoft Visual FoxPro, or Microsoft Visual Basic. Beyond this level, this certification has been replaced with the MCPD already mentioned.

- **MCDBA (Microsoft Certified Database Administrator)**—The MCDBA credential reflects the skills required to implement and administer Microsoft SQL Server databases. To become an MCDBA, you must pass a total of three core exams and one elective exam. The core exams involve SQL Server administration, SQL Server design, and networking systems. Beginning with SQL Server 2005, this certification has been replaced with the MCITP: Database Developer and the MCITP: Database Administrator certifications.
- **MCT (Microsoft Certified Trainer)**—Microsoft Certified Trainers are deemed able to deliver elements of the official Microsoft curriculum, based on technical knowledge and instructional ability. Therefore, it is necessary for an individual seeking MCT credentials (which are granted on a course-by-course basis) to pass the related certification exam for a course and complete the official Microsoft training in the subject area, as well as to demonstrate an ability to teach.

  This teaching skill criterion may be satisfied by proving that you have already attained training certification from Novell, Banyan, Lotus, the Santa Cruz Operation, or Cisco, or by taking a Microsoft-sanctioned workshop on instruction. Microsoft makes it clear that MCTs are important cogs in the Microsoft training channels. Instructors must be MCTs before Microsoft allows them to teach in any of its official training channels, including the Certified Technology Education Centers (CTEC) and its online training partner network.

After a Microsoft product becomes obsolete, MCPs typically have to recertify on current versions. (If individuals do not recertify, their certifications become invalid; a current exception to this rule is the MCSE on Windows NT 4.0.) Because technology keeps changing and new products continually supplant old ones, this recertification requirement should come as no surprise.

The best place to keep tabs on the various certification programs is on the Web. The URL for these programs is http://www.microsoft.com/learning/default.mspx. But the Microsoft website changes often, so if this URL doesn't work, try using the Search tool on the Microsoft site with "MCP," "MCTS," or the quoted phrases "Microsoft Certified Professional" or "Microsoft Certified Technology Specialist" as a search string. This can help you find the latest and most accurate information about Microsoft's certification programs.

About the Exam and Content Areas

Exam 70-640: Windows Server 2008 Active Directory, Configuring, includes a variety of content. For specifics on the exam, check the exam guide on the Microsoft website at http://www.microsoft.com/learning/en/us/exams/70-640.mspx.

The broad topic areas covered by the exam include the following:

- **Configuring Domain Name System (DNS) for Active Directory**—You should be able to configure DNS zones, DNS server settings, zone transfers, and replication.
- **Configuring the Active Directory Infrastructure**—You are expected to be able to configure Active Directory forests, domains, trusts, sites, replication, global catalog, and operations masters.
- **Configuring Additional Active Directory Server Roles**—You are expected to be able to configure Windows Server 2008 as a Server Core domain controller and a read-only domain controller, and to use the new Server Manager console to configure services related to Active Directory in Windows Server 2008.
- **Creating and Maintaining Active Directory Objects**—You should be able to configure and maintain Active Directory accounts, including automatic creation of user and group accounts. You should also be able to configure Group Policy objects (GPO), including creating and applying GPOs and configuring GPO templates, software deployment GPOs, account policies, and audit policies.
- **Maintaining the Active Directory Environment**—You should be familiar with how to monitor and maintain Active Directory and be able to recover from various types of failures.
- **Configuring Active Directory Certificate Services**—You must be able to install Certificate Services and configure server settings, certificate templates, and certificate enrollments and revocations in Active Directory.

Each of the task areas represents important components of Active Directory management that an individual responsible for the task must be familiar with. You will be able to plan and implement an Active Directory installation and perform the essential day-to-day management and troubleshooting tasks.

How to Prepare for the Exam

Preparing for any Windows Server 2008–related exam requires that you obtain and study materials designed to provide comprehensive information about the product and its capabilities that will appear on the specific exam for which you are preparing. The following list of materials will help you study and prepare:

- The Windows Server 2008 product DVD-ROM, which includes comprehensive online documentation and related materials; it should be a primary resource when you are preparing for the test.
- The exam preparation materials, practice tests, and self-assessment exams on the Microsoft Certified Professional and Office Specialist Exams page at http://www.microsoft.com/learning/mcpexams/default.mspx; the Testing Innovations page (http://www.microsoft.com/learning/mcpexams/policies/innovations.mspx) offers examples of the new question types found on the Windows Server 2008 MCTS and MCITP exams. Find the material, download it, and use it!
- The exam-preparation advice, practice tests, questions of the day, and discussion groups on the ExamCram.com e-learning and certification destination website (http://www.informit.com/imprint/index.aspx?st=61087).

In addition, you'll probably find any or all of the following materials useful in your quest for Active Directory configuration expertise:

- **Microsoft training kits**—Microsoft Press offers a training kit that specifically targets Exam 70-640. For more information, visit http://www.microsoft.com/MSPress/books/11754.aspx. This training kit contains information useful in preparing for the test.
- **Microsoft TechNet Subscriptions**—This Microsoft resource delivers comprehensive resources that assist IT professionals in resolving problems and issues, implementing technologies, and enhancing their skills. Included are product facts, technical notes, tools and utilities, and access to training materials for all aspects of Windows Server 2008, Windows Vista, and other Microsoft products. Beta software and evaluation versions of released software packages are also included. A subscription to TechNet costs anywhere from $349 to $999 per year, but it is well worth the price. Visit http://technet.microsoft.com/en-us/subscriptions/default.aspx and check out the information under the TechNet Plus Subscriptions menu entry for more details.

- **Study guides**—Several publishers, including Que, offer Windows Server 2008 titles. Que Certification includes the following:
  - **The *Exam Cram* series**—These books provide information about the material you need to know to pass the tests.
  - **The *Exam Prep* series**—For some Microsoft exams, Que also offers *Exam Prep* books, which provide a greater level of detail than the *Exam Cram* books and are designed to teach you everything you need to know from an exam perspective. Each book comes with a CD-ROM that contains interactive practice exams in a variety of testing formats.
- **Multimedia**—The MeasureUp Practice Tests CD-ROM that comes with each *Exam Cram* and *Exam Prep* title features a powerful, state-of-the-art test engine that prepares you for the actual exam. MeasureUp Practice Tests are developed by certified IT professionals and are trusted by certification students around the world. For more information, visit www.measureup.com.
- **Classroom training**—CTECs and third-party training companies (such as Learning Tree International, Global Knowledge, New Horizons, triOS College, and others) offer classroom training on Windows Server 2008. Although such training runs upward of $350 per day in class, most of the individuals lucky enough to partake find it to be quite worthwhile.
- **Other publications**—There's no shortage of materials available about Active Directory configuration. The resource sections in Appendix A, "Need to Know More?" should give you an idea of where you should look for further discussion.

You cannot adequately prepare for this exam or other Microsoft certification exams by simply rote-memorizing terms and definitions. You need to be able to analyze a scenario and answer by combining various knowledge points from various topic areas. Successfully completing this exam requires a great deal of thought and analysis to properly choose the "best" solution from several "viable" solutions in many cases.

As stated and restated, this exam is best prepared for by doing. You must work with Active Directory and all of its features to be comfortable with the material being addressed by the exam.

Taking a Certification Exam

After you've prepared for your exam, you need to register with a testing center. Each computer-based MCP exam costs $125, and if you don't pass, you may retest for an additional $125 for each try. In the United States and Canada, all tests after January 1, 2008, are administered by Prometric. You can sign up for an exam through the company's website at securereg3.prometric.com, or you can register by phone at 800-755-3926 (within the United States and Canada) or at 410-843-8000 (outside the United States and Canada).

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

To schedule an exam, call the number or visit the web page at least one day in advance. To cancel or reschedule an exam, you must call before 7 p.m. Pacific Standard Time the day before the scheduled test time (or you may be charged, even if you don't appear to take the test). When you want to schedule a test, have the following information ready:

- Your name, organization, and mailing address.
- Your Microsoft Test ID. (Inside the United States, this means your Social Security Number and in Canada, it means your Social Insurance Number. Citizens of other nations should call ahead to find out what type of identification number is required to register for a test.)
- The name and number of the exam you want to take.
- A method of payment. Besides the methods already mentioned, you might be able to purchase a voucher online before registering.

After you sign up for a test, you are informed as to when and where the test is scheduled. Try to 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.

All exams are completely closed book. In fact, you are not permitted to take anything into the test area, but you are furnished with a blank sheet of paper and a pen, or in some cases, an erasable plastic sheet and an erasable pen. Immediately write down on that sheet of paper all the information you've memorized for the test. In *Exam Cram* books, this information appears on a tearcard inside the front cover of each book. You are allowed some time to compose yourself,

record this information, and take a sample orientation exam before you begin the real thing. It's best to take the orientation test before taking your first exam, but because they're all more or less identical in layout, behavior, and controls, you probably don't need to do this more than once.

When you complete a Microsoft certification exam, the software tells you whether you've passed or failed. If you need to retake an exam, you have to schedule a new test with Prometric and pay another $125.

NOTE

The first time you fail a test, you can retake it the next day. However, if you fail a second time, you must wait 14 days before retaking that test. The 14-day waiting period remains in effect for all retakes after the second failure.

What This Book Will Do

This book is designed to be read as a pointer to the areas of knowledge you will be tested on. In other words, you might want to read this book one time just to get insight into how comprehensive your knowledge of this topic is. The book is also designed to be read shortly before you go for the actual test. You can use this book to get a sense of the underlying context of any topic in the chapters or to skim-read for Exam Alerts, bulleted points, summaries, and topic headings.

This book draws on material from Microsoft's own listing of knowledge requirements, from other preparation guides, and from the exams. It also draws from a battery of technical websites, as well as from my own experience with Microsoft servers and the exam. The goal is to walk you through the knowledge you will need. By reading this book, you will gain from the experience of real-world professional development.

What This Book Will Not Do

This book will not teach you everything you need to know about Active Directory in Windows Server 2008. The scope of the book is exam preparation. It is intended to ramp you up and give you confidence heading into the exam. This book is not intended as an introduction to Active Directory configuration. It reviews what you need to know before you take the test, with its fundamental purpose dedicated to reviewing the information needed on the Microsoft certification exam.

This book uses a variety of teaching and memorization techniques to analyze the exam-related topics and to provide you with everything you need to know to pass the test.

About This Book

Read this book from front to back. You won't be wasting your time because nothing written here is a guess about an unknown exam. I have had to explain certain underlying information on such a regular basis that I have included those explanations here.

After you have read this book, you can brush up on a certain area by using the index or the table of contents to go straight to the topics and questions you want to re-examine. I have tried to use the headings and subheadings to provide outline information about each given topic. After you have been certified, you will find this book useful as a tightly focused reference and an essential foundation of Active Directory configuration and management.

Each *Exam Cram* chapter follows a regular structure and offers graphical cues about especially important or useful material. The structure of a typical chapter is as follows:

- **Opening hotlists**—Each chapter begins with lists of the terms you need to understand and the concepts you need to master before you can be fully conversant in the chapter's subject matter. The hotlists are followed with a few introductory paragraphs, setting the stage for the rest of the chapter.
- **Topical coverage**—After the opening hotlists, each chapter covers the topics related to the chapter's subject.
- **Exam Alerts**—Throughout the text, the material that is most likely to appear on the exam is highlighted by using a special Exam Alert that looks like this:

EXAM ALERT

This is what an Exam Alert looks like. An Exam Alert stresses concepts, terms, or best practices that will most likely appear in at least one certification exam question. For that reason, any information presented in an Exam Alert is worthy of unusual attentiveness on your part.

Even if material is not flagged as an Exam Alert, all the content in this book is associated in some way with test-related material. What appears in the chapter content is critical knowledge.

- **Notes**—This book is an overall examination of Active Directory configuration, management, and troubleshooting. As such, it delves into many aspects of computer networks. Where a body of knowledge is deeper than the scope of the book, this book uses Notes to indicate areas of concern.

NOTE

Cramming for an exam will get you through a test, but it will not make you a competent Active Directory professional. Although you can memorize just the facts you need to become certified, your daily work in the field will rapidly put you in water over your head if you do not know the underlying principles.

- **Tips**—This book provides Tips that will help you build a better foundation of knowledge or to focus your attention on an important concept that reappears later in the book. Tips provide a helpful way to remind you of the context surrounding a particular area of a topic under discussion.

TIP

This is how Tips are formatted. Keep your eyes open for them, and you'll become an Active Directory configuration guru in no time!

- **Practice questions**—These present a short list of test questions related to the specific chapter topic. Following each question is an explanation of both correct and incorrect answers. The practice questions highlight the areas that are the most important on the exam.

The bulk of this book follows this chapter structure, but I would like to point out a few other elements:

- **Details and resources**—Appendix A at the end of this book is titled "Need to Know More?" This appendix provides direct pointers to Microsoft and third-party resources offering more details on each chapter's subject. If you find a resource you like in this collection, use it, but don't feel compelled to use all the resources. On the other hand, I recommend only resources that I use regularly, so none of my 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 would-be MCTSs and MCITPs might find hard to justify).

- **Glossary**—This book has an extensive glossary of important terms used throughout the book.
- **The Cram Sheet**—This appears as a tearcard inside the front cover of this *Exam Cram* book. It is a valuable tool that represents a collection of the most difficult-to-remember facts and numbers you should memorize before taking the test. Remember, you can dump this information out of your head onto a piece of paper as soon as you enter the testing room. This tearcard has facts that require brute-force memorization. You need to remember this information only long enough to write it down when you walk into the test room. Be advised that you will be asked to surrender all personal belongings other than pencils before you enter the exam room.

  You might want to look at the Cram Sheet in your car or in the lobby of the testing center just before you walk into the testing center. It is divided into exam objective headings, so you can review the appropriate parts just before each test.

7

CHAPTER 7

Group Policy and Active Directory Security

Terms You'll Need to Understand

- ✓ Account lockout
- ✓ Account policies
- ✓ Auditing
- ✓ Auditpol.exe
- ✓ Fine-grained password policies
- ✓ Password settings objects (PSO)

Concepts/Techniques You'll Need to Master

- ✓ Managing security configurations
- ✓ Configuring account policies
- ✓ Configuring fine-grained password policies
- ✓ Using Group Policy to configure auditing policies
- ✓ Using `Auditpol.exe` to configure auditing policies

You have seen how Group Policy works and how to set up Group Policy objects (GPO) to configure various aspects of the Windows computing environment. You have also learned about Group Policy succession and how you can modify the sequence in which GPOs are applied and its effect when policy settings conflict with one another. You have also read about the use of Group Policy to maintain a consistent software environment, where users and computers receive a well-regulated set of software applications that can be modified and upgraded as required, as well as the removal of outdated software. This chapter focuses on the use of Group Policy to create and enforce a secure computing environment that protects your computers and data from whatever the bad guys might attempt to throw at you.

Use of Group Policy to Configure Security

You can use Group Policy to manage security settings quite effectively on a Windows Server 2008 network. An enhanced range of security options is available, with settings designed for both user and computer configuration. Microsoft continues to expand the available range of security policies, compared to those included with previous versions of Windows Server. The most significant addition to security settings in Windows Server 2008 is that of fine-grained password policies, which enable you to set different password policies for different portions of your AD DS domain.

Group Policy in Windows Server 2008 includes a large range of security options designed for both user and computer configuration. As you can see in Figure 7.1, most of these security settings are applied to the Computer Configuration section in the Group Policy Management Editor. This section is mainly concerned with account policies.

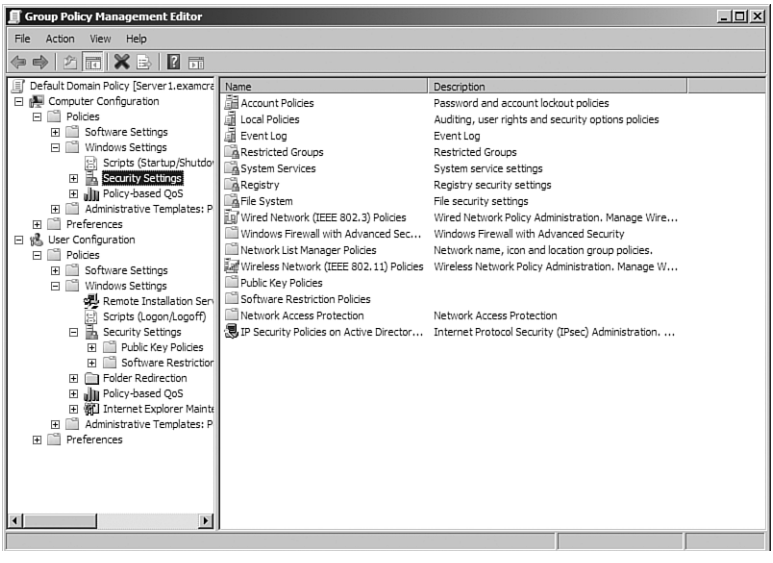

FIGURE 7.1 Group Policy includes both computer- and user-based security settings.

Configuring Account Policies

The *Account Policies* node contains settings related to user accounts, including the password policy, account lockout policy, and Kerberos policy. Before looking at the new Windows Server 2008 feature of fine-grained password policies, this section examines these policies and how to configure them, in general. It briefly introduces each of these concepts in the following sections.

Domain Password Policies

You can use domain-based Group Policy to configure password policy settings that help to protect users of Windows 2000/XP/Vista client computers. The options available in Windows Server 2008 are similar to those introduced in Windows 2000 and continued in Windows Server 2003. Password policies are generally intended to make passwords more difficult for intruders to discover. Figure 7.2 shows the available password policies and their default settings.

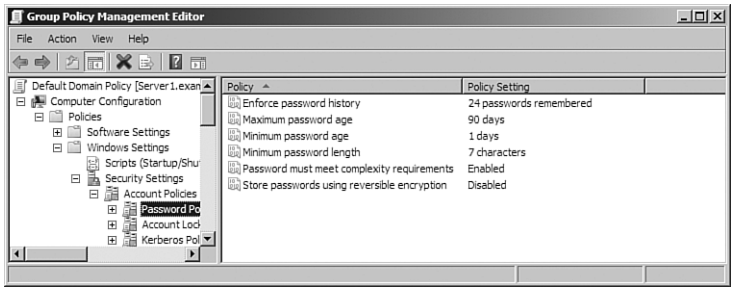

FIGURE 7.2 Windows Server 2008 provides default values for the available password policies.

The following password policy settings are available:

- **Enforce Password History**—Determines the number of passwords remembered by AD DS for each user. Values range from 0 to 24. A user cannot reuse a password retained in the history list. A value of 0 means that no password history is retained and a user can reuse passwords at will. Windows Server 2008 continues with the default of 24 established with Windows Server 2003 SP1.
- **Maximum Password Age**—Determines the number of days that a user can use a password before being required to specify a new one. Values range from 0 to 999. A value of 0 means that a user is never required to change his password. The default is 90 days.
- **Minimum Password Age**—Determines the minimum number of days a password must be used before it can be changed. Values range from 0 to 999 days and must be less than the maximum password age. A value of 0 allows the user to immediately change a new password. This value would allow a user to cycle through an entire history list of passwords in a short time—in other words, repeatedly changing a password so he could reuse his old password. This obviously defeats the purpose of enforcing password history. The default is 1 day.
- **Minimum Password Length**—Determines the minimum number of characters that can make up a password. Values range from 0 to 14. A value of 0 permits a blank password. Use a setting of 10 or higher for increased security. The default is 7 characters.
- **Password Must Meet Complexity Requirements**—Stipulates that a password must meet complexity criteria, as follows: The password cannot contain the user account name or full name, or parts of the name that exceed two consecutive characters. It must contain at least three of the following four items:

- English lowercase letters
- English uppercase letters
- Numerals
- Nonalphanumeric characters, such as $; [ ] { } ! .

- **Store Passwords Using Reversible Encryption**—Determines the level of encryption used by Windows Server 2008 for storing passwords. Enabling this option reduces security because it stores passwords in a format that is essentially the same as plain text. This option is disabled by default. You should enable this policy only if needed for clients who cannot use normal encryption, such as those using Challenge Handshake Authentication Protocol (CHAP) authentication or Internet Information Services (IIS) Digest Authentication.

To configure these policies, expand the Computer Configuration node of the appropriate GPO, as shown in Figure 7.2. Right-click the desired policy and choose Properties. Then configure the appropriate value and click OK. Each policy setting also has an Explain tab that provides additional information on the policy setting and its purpose.

EXAM ALERT

Password policies are unique in that they apply only when configured in a domain-based GPO. Although they appear in other GPOs, any configuration in GPOs linked to other containers is ignored.

Account Lockout

A cracked user account password jeopardizes the security of the entire network. The *account lockout* policy is designed to lock an account out of the computer if a user (or intruder attempting to crack the network) enters an incorrect password a specified number of times, thereby limiting the effectiveness of dictionary-based password crackers. The account lockout policy contains the following settings:

- **Account Lockout Duration**—Specifies the number of minutes that an account remains locked out. Every account except for the default Administrator account can be locked out in this manner. You can set this value from 0 to 99999 minutes, or about 69.4 days. A value of 0 means that accounts that have exceeded the specified number of failed logon attempts are locked out indefinitely until an administrator unlocks the account.

- **Account Lockout Threshold**—Specifies the number of failed logon attempts that can occur before the account is locked out. You can set this value from 0 to 999 failed attempts. A value of 0 means that the account will never be locked out. Best practices recommend that you should never configure a setting of 0 here.
- **Reset Account Lockout Counter After**—Specifies the number of minutes to wait after which the account lockout counter is reset to 0. You can set this value from 1 to 99999.

When you configure this policy, Windows Server 2008 sets default values for the account lockout settings. To configure an account lockout policy, right-click any of the three values and choose Properties, and then accept the default provided or specify a value of your choice. As shown in Figure 7.3, Windows suggests default values for the other two policy settings. Click OK to define the policy settings and set these defaults. If you want to change the other settings, right-click the appropriate settings and choose Properties, and then enter the desired value.

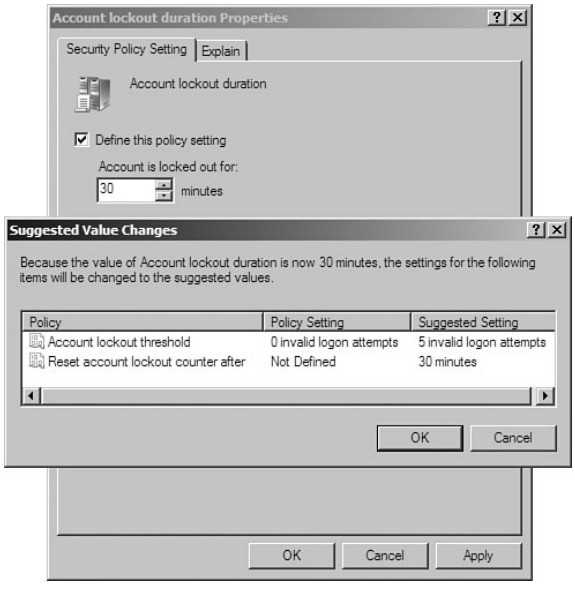

FIGURE 7.3 When you define an account lockout policy, Windows suggests defaults for the other two lockout policy settings.

Unlocking an Account

When a user account is locked out because of too many incorrect attempts at entering a password, it is simple for an administrator or user who is delegated the task to unlock it. Right-click the user account in Active Directory Users and

Computers and choose Properties. On the Account tab of the user's Properties dialog box, the Unlock Account check box should display a message stating `This account is currently locked out on this Active Directory Domain Controller`. Select the check box, and then click OK or Apply.

Kerberos Policy

The Kerberos Policy subnode contains settings that enforce use logon restrictions according to validation requests made to the Kerberos Key Distribution Center (KDC) against the user rights policy of the user account. By default, the policies in this section are enabled. They define the maximum lifetime for user and service tickets as well as the maximum tolerance for computer clock synchronization.

CAUTION

Kerberos policies generally do not appear on Exam 70-640. However, you should be aware of the Maximum Tolerance for Computer Clock Synchronization policy setting. This setting specifies the maximum time difference in minutes between the domain controller clock and that on a client computer attempting authentication. If the clocks differ by more than the specified amount (five minutes by default), authentication fails.

Fine-Grained Password Policies

Active Directory domains in Windows 2000 and Windows Server 2003 permitted only a single password and account lockout policy, defined at the domain level. If an organization wanted different password policy settings for a specified group of users, an administrator had to create a new domain or use a third-party custom password filter. Windows Server 2008 introduces the concept of *fine-grained password policies*, which enable you to apply granular password and account lockout policy settings to different sets of users within the same domain. For example, you can apply stricter policy settings to accounts associated with users who have access to classified or restricted information, such as legal and product research departments. At the same time, you can maintain more relaxed settings for accounts of other users where these types of information are not available.

To configure a fine-grained password policy, you must be a member of the Domain Admins group, and the domain functional level must be set to Windows Server 2008. You can also delegate control of the task to other users if required.

Fine-grained password policies are stored in AD DS by means of two new object classes that are defined in the schema:

- **Password Settings Container**—Created by default under the domain's System container, the Password Settings Container stores the *password settings objects (PSO)* for the domain.
- **Password Settings Object**—Holds attributes for all the password policy and account lockout policy settings, as defined earlier in this section. It also contains a multivalued link attribute that links the PSO to users or groups, and an integer precedence value that resolves conflicts if multiple PSOs are applied to the same user or group.

You can link a PSO to a user, global security group, or InetOrgPerson object that is in the same domain. Note that if you link a PSO to a distribution group or a group with a different scope, the PSO is ignored. If multiple PSOs are linked to a single user or group because of membership in multiple groups, only one PSO can be applied; settings cannot be merged between PSOs.

EXAM ALERT

Remember the prerequisites for configuring and applying fine-grained password policies. You must be a member of the Domain Admins group, the domain functional level must be set to Windows Server 2008, and the policies must be applied to the users or global security groups that need them.

Password Settings Precedence

If more than one PSO is linked to a user or group, the PSO that applies is determined by the precedence attribute, which is associated with each PSO and has an integer value of 1 or greater. The lower the precedence attribute, the higher the priority of a given PSO; for example, a PSO with a precedence value of 3 overrides another PSO with a precedence value of 5.

The following rules determine the resultant PSO that is applied to a user or group when multiple PSOs are present:

- If a PSO is directly linked to the user object, it prevails. Should more than one PSO be linked directly to the user, the PSO with the lowest precedence value prevails, and a warning message is logged to the event log.
- If no PSO is linked directly to the user object, all PSOs applied to the user according to membership in global security groups are evaluated, and the PSO with the lowest precedence value prevails. If more than one PSO with the same precedence value is present, the PSO that is obtained first is used.

- If no PSO is linked to either the user object or any global security groups it is a member of, the settings in the Default Domain Policy GPO are applied.

NOTE

You cannot apply a PSO directly to an organizational unit (OU). If you want to apply consistent password settings to all users in an OU, you should add these users to a global security group and apply the PSO to this group. If you move a user from one OU to another with different password security needs, you must update this user's group membership to reflect the change.

TIP

It is recommended that you specify a unique precedence value for each PSO. This simplifies troubleshooting of password precedence settings problems. But remember that setting a PSO for a user means this PSO takes precedence over PSOs linked to groups, regardless of their precedence setting.

Configuring Fine-Grained Password Policies

As already stated, you must be a member of the Domain Admins group to create and manage PSOs. You can use the ADSI Edit utility to configure a fine-grained password policy. This involves specifying values for all the Password Policy and Account Lockout Policy settings described earlier in this chapter. This tool was introduced in Chapter 4, "Configuring Additional Active Directory Roles." Perform the following steps:

1. Click Start, Run, type **`adsiedit.msc`**, and then press Enter.
2. If the domain name is not visible in the console tree, right-click ADSI Edit and choose Connect To. If `Default Naming Context` and your domain name are visible in the Connection Settings dialog box, accept them. Otherwise, type the fully qualified domain name (FQDN) of your domain. Then click OK.
3. Expand your domain name to locate the `CN=System` container, and then expand this container to locate the `CN=Password Settings Container` object.
4. Select this container to display any PSOs that are configured in the domain in the Details pane.
5. Right-click this container and choose New, Object. This starts a wizard that enables you to define your PSO.

6. In the Create Object dialog box, the `msDS-PasswordSettings` object class is the only available class. Ensure that it is selected, and then click Next.
7. Provide a descriptive value for your PSO, as shown in Figure 7.4, and then click Next.

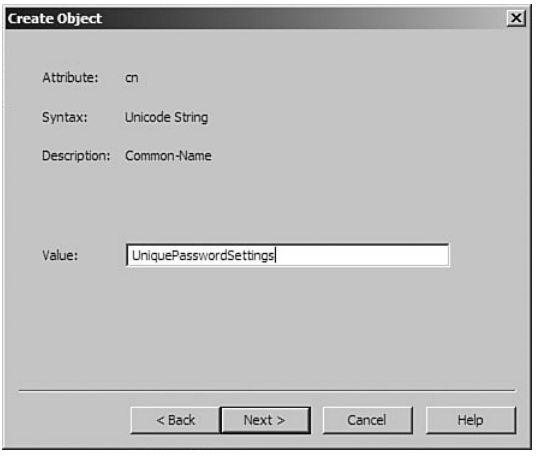

FIGURE 7.4 Provide a descriptive value that helps you to identify the PSO later.

8. Type a value for the Password Settings Precedence, and then click Next.
9. For Password Reversible Encryption Status for User Accounts, type **`False`** unless you need reversible encryption, and then click Next.
10. Type a value for the password history length, and then click Next.
11. To require password complexity, type **`True`**, and then click Next.
12. Specify a minimum password length, and then click Next.
13. For the Minimum Password Age for User Accounts value, type a value in the format *`days:hours:minutes:seconds`* (for example, **`1:00:00:00`**), and then click Next.
14. Type a value for Maximum Password Age for User Accounts in the same format, and then click Next.
15. Type a value for the lockout threshold (number of incorrect passwords before account locks out), and then click Next.
16. Type a value for the lockout observation window (time for resetting lockout counter) in the same format as already described (for example, **`00:00:30:00`** for 30 minutes), and then click Next.

17. Type a value for the lockout duration in the same format, and then click Next.
18. If you want to define additional optional attributes, click More Attributes. Otherwise, click Finish to complete the creation of the PSO.

To apply the PSO to a user or group, proceed as follows:

1. Open Active Directory Users and Computers and select Advanced Features under the View menu.
2. In the console tree, expand System, and then select Password Settings Container. This displays the PSO in the Details pane.
3. Right-click the PSO and choose Properties.
4. Select the Attribute Editor tab. As shown in Figure 7.5, this tab displays the values of all attributes that have been configured for the PSO, including those set when you created the PSO.

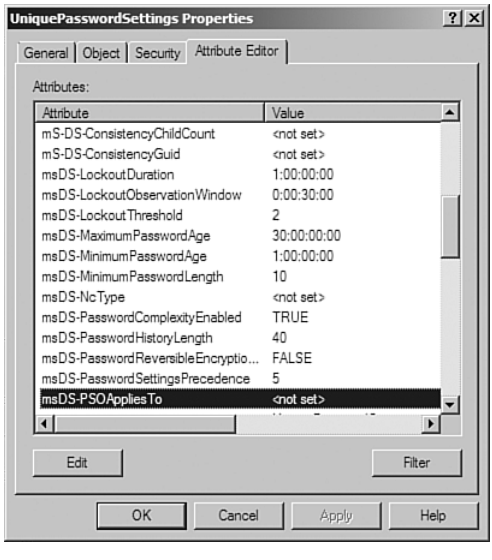

FIGURE 7.5 The Attribute Editor tab of the PSO's Properties dialog box includes the values of the password and lockout attributes that you configured.

5. Scroll to select the `msDS-PSOAppliesTo` attribute, and then click Edit.

6. On the Multi-valued Distinguished Name With Security Principal Editor dialog box that displays, click Add Windows Account, type the user or group name, and then click OK. As shown in Figure 7.6, the name you added is displayed in this dialog box. You can also add a user or group with its LDAP distinguished name (DN) by clicking the Add DN button.

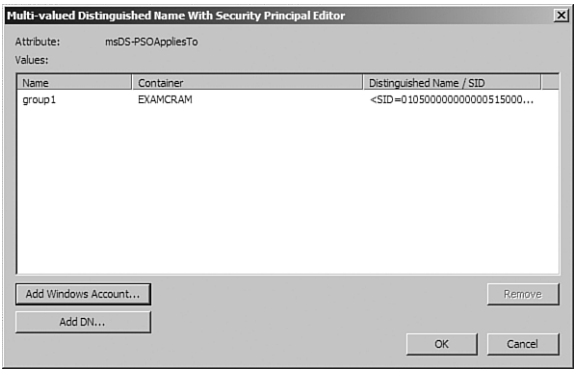

FIGURE 7.6 Specifying a user or group that will receive the password policy.

7. Click OK. The security identifier (SID) of the user or group appears in the Value column of the Attribute Editor tab. You can repeat this process as many times as needed to link the PSO to additional users or groups.
8. Click OK to close the PSO's Properties dialog box.

NOTE

You can also use the `ldifde` utility to create a PSO and specify users or groups to which the PSO can apply. Chapter 5, "Active Directory Objects and Trusts," introduced this utility. Refer to "Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration" in Appendix A, "Need to Know More?" and select the links provided for steps 1 and 2 for additional details.

Managing Fine-Grained Password Policies

You can perform several additional managerial tasks on your PSO, as follows:

- **Editing policy settings**—As described in the previous section, access the Attribute Editor tab of the PSO's Properties dialog box. Select the policy setting to be edited and click Edit. Then specify the desired value in the Editor dialog box that appears.

- **Modify the PSO's precedence value**—In the Attribute Editor tab of the PSO's Properties dialog box, select the `msDS-PasswordSettingsPrecedence` value, click Edit, and then specify the desired value in the Integer Attribute Editor dialog box that appears.
- **Delete the PSO**—If you no longer need the PSO, select it in the Details pane of Active Directory Users and Computers and press the Delete key (or right-click it and choose Delete). Click Yes in the confirmation message box that appears. The policy settings for any users or groups employing this PSO revert to the settings in a lower-priority PSO or to the Default Domain Policy GPO if no other PSO exists.

Viewing the Resultant PSO

As already stated, a PSO configured for the user takes priority over one that is configured for a group to which the user belongs, and group-based PSOs are applied according to the precedence value. If you have configured a large number of PSOs, troubleshooting their application can become problematic. To facilitate this process, you can view which PSO is applying to a user or group. Proceed as follows:

1. In Active Directory Users and Computers, ensure that Advanced Features is selected.
2. Select the Users container or the OU of the desired user account to display the user account in the Details pane.
3. Right-click the user account and choose Properties.
4. Select the Attribute Editor tab, and then click Filter. In the options list that appears, ensure that Show Attributes/Optional and Show Read-Only Attributes/System-Only are checked.
5. Scroll the attribute list to locate `msDS-ResultantPSO`. The value of this attribute displays the DN of the effective PSO, as shown in Figure 7.7. If it displays `<not set>`, the password settings in the Default Domain Policy GPO are in effect for this account. Click View to see the complete DN.

For additional information on fine-grained password policies, including some recommended scenarios for applying these policies, refer to "Step-by-Step Guide for Fine-Grained Password and Account Lockout Policy Configuration" in Appendix A. Links in this appendix also provide additional information on the available attributes and their permitted values.

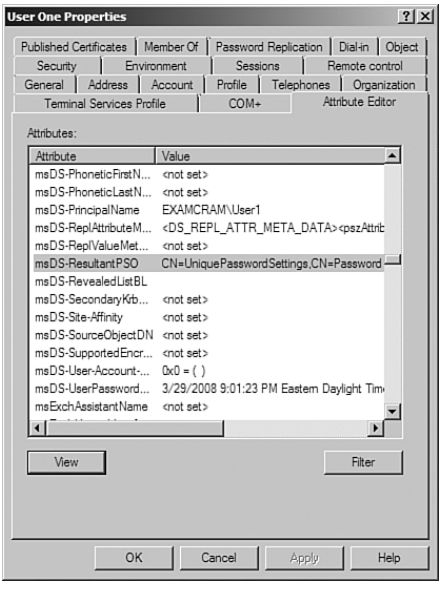

FIGURE 7.7 You can view the effective PSO for a user or group.

Security Options

Besides account policies, the Security Settings subnode of Computer Configuration includes a large range of additional security-related policy settings. These settings are summarized here:

- **Local Policies**—Includes audit policies, discussed later in this chapter, and user rights assignment, discussed in Chapter 6, "Configuring and Troubleshooting Group Policy." The Security Options subnode within this node includes a large set of policy options, as shown in Figure 7.8, that are important in controlling security aspects of the computers to which the GPO applies. Several of the more important options that you should be familiar with are as follows:
  - **Accounts: Rename Administrator Account**—This option renames the default administrator account to a value you specify. Intruders cannot simply look for "Administrator" when attempting to crack your network.
  - **Interactive Logon: Do Not Display Last User Name**—Enable this option to prevent the username of the last logged-on user from appearing in the Logon dialog box, thus preventing another individual from seeing a username. This can also reduce lockouts.

- **Interactive Logon: Do Not Require CTRL+ALT+DEL**—When enabled, a user is not required to press Ctrl+Alt+Delete to obtain the Logon dialog box. Disable this policy in a secure environment to require the use of this key combination. Its use prevents rogue programs such as Trojan horses from capturing usernames and passwords.
- **Interactive Logon: Require Smart Card**—When enabled, users must employ a smart card to log on to the computer.
- **User Account Control**—Several policy settings determine the behavior of the UAC prompt for administrative and nonadministrative users, including behavior by applications that are in secure locations on the computer, such as `%ProgramFiles%` or `%Windir%`.

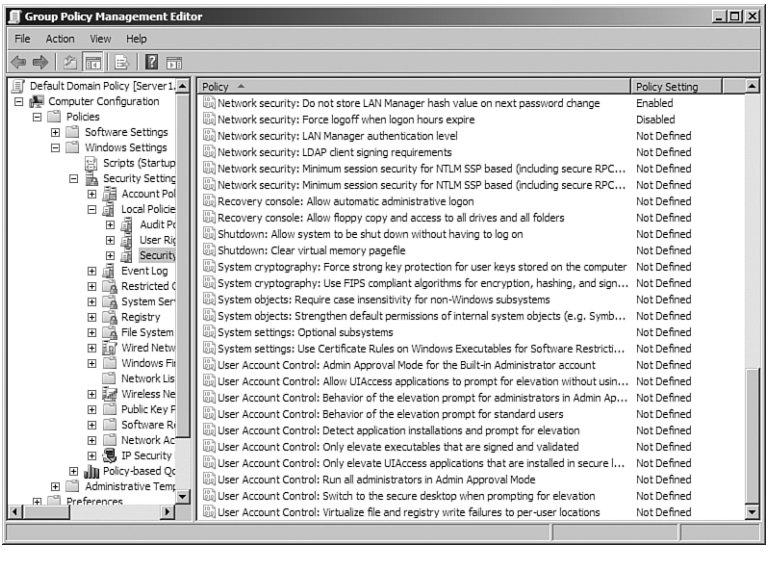

FIGURE 7.8 You can configure numerous local security policy settings with Group Policy in Windows Server 2008.

For more information on the policy settings in this node, refer to "Domain Controller and Member Server Policy Settings" in Appendix A.

- **Event Log**—Configuration options for the Event Viewer logs, including log sizes and action taken when an event log is full.
- **Restricted Groups**—Determines who can belong to certain groups, as discussed in Chapter 6.

- **System Services**—Enables you to configure system services properties, such as startup type, and restrict users from modifying these settings.
- **Registry**—Enables you to control the permissions that govern who can access and edit portions of the Registry.
- **File System**—Enables you to configure permissions on folders and files and prevent their modification.
- **Wired Network (IEEE 802.3) Policies**—Enables you to specify the use of IEEE 802.1X authentication for network access by Windows Vista computers, including the protocol to be used for network authentication.
- **Windows Firewall with Advanced Security**—Enables you to configure properties of Windows Firewall for domain, private, and public profiles. You can specify inbound and outbound connection rules as well as monitoring settings.
- **Network List Manager Policies**—Enables you to control the networks that computers can access and their location types, such as public and private (which automatically specifies the appropriate firewall settings according to location type). You can also specify which networks a user is allowed to connect to.
- **Wireless Network (IEEE 802.11) Policies**—Enables you to specify wireless settings, such as enabling 802.1X authentication and the preferred wireless networks that users can access.
- **Public Key Policies**—Enables you to configure public key infrastructure (PKI) settings. Chapter 9, "Active Directory Certificate Services," discusses several of these policies.
- **Software Restriction Policies**—Enables you to specify which software programs users can run on network computers, which programs users on multiuser computers can run, and the execution of email attachments. You can also specify whether software restriction policies apply to certain groups such as administrators.
- **Network Access Protection**—Network Access Protection (NAP) is a new Windows Server 2008 feature that enables you to define client health policies that restrict access to your network by computers that lack appropriate security configurations. The NAP policies enable you to specify settings for client user interface items, trusted servers, and servers used for enforcement of client computer security health status.

- **IP Security Policies on Active Directory**—Controls the implementation of IP Security (IPSec) as used by the computer for encrypting communications over the network.

You can obtain additional information on many of these policy settings in the Windows Server 2008 Help and Support and from "Security Settings Overview for GPMC" in Appendix A.

Additional Security Configuration Tools

Windows Server 2008 includes the following additional tools that are useful in configuring and maintaining the security of your AD DS network:

- **Security Configuration Wizard**—This wizard assists you in maintaining the security of your servers and checks for vulnerabilities that might appear as server configurations change over time. It is particularly useful in maintaining the security of servers hosting roles that are not installed using Server Manager, such as SQL Server and Exchange Server, as well as servers that host non-Microsoft applications. Microsoft also includes a command-line version, `scwcmd.exe`, which is useful in configuring Server Core computers.
- **Security Templates snap-in**—From this snap-in, you can save a custom security policy that includes settings from the various subnodes of the Security Settings node of Computer Configuration discussed in the preceding settings. It is most useful in defining a security configuration for standalone servers that are not members of a domain.
- **Security Configuration and Analysis snap-in**—This snap-in enables you to analyze and configure local computer security. You can compare security settings on the computer to those in a database created from the Security Templates snap-in and view any differences that you find. You can then use this database to configure the computer's security so that it matches the database settings.

NOTE

Unlike previous versions of Windows Server, Windows Server 2008 does not include predefined security templates, such as the Compatible, Secure Server, and High Secure Server templates included with Windows Server 2003. However, you can use the Security Templates snap-in to create a custom template that you can use for configuring security settings on standalone servers or servers in another forest.

These security tools are most useful in situations involving standalone computers and servers running custom applications and are not emphasized on Exam 70-640. For more information on these tools, refer to "Server Security Policy Management in Windows Server 2008" in Appendix A.

Auditing of Active Directory Services

Auditing enables you to track actions performed by users across the domain, such as logging on and off or accessing files and folders. When you create and apply an auditing policy, auditable events are recorded in the Security log of the computer where they happen. You can then use Event Viewer to view any computer's Security log by connecting to the required computer.

New Features of Active Directory Auditing

Windows Server 2008 introduces a new command-line tool, `auditpol.exe`, as well as subcategories in the Audit Directory Service Access category. In previous versions of Windows Server, a single Directory Service Access category controlled the auditing of all directory service events. In Windows Server 2008, four subcategories of directory service access are available:

- **Directory Service Access**—Tracks all attempts at accessing AD DS objects whose system access control lists (SACL) have been configured for auditing. This includes deletion of objects.
- **Directory Service Changes**—Tracks modifications to AD DS objects whose SACLs have been configured for auditing. The following actions are included:
  - When an attribute of an object has been modified, the old and new values of the attribute are recorded in the Security log.
  - When a new object is created, values of their attributes including new attribute values are recorded in the Security log. This includes objects moved from another domain.
  - When objects are moved from one container to another, the distinguished names of the old and new locations are recorded in the Security log.
  - When objects are undeleted, the location in which they are placed is recorded in the Security log. Any added, modified, or deleted attributes are recorded also.

- **Directory Service Replication**—Tracks the beginning and end of the synchronization of a replica of an Active Directory naming context.
- **Detailed Directory Service Replication**—Tracks additional AD DS replication events, including the establishment, removal, or modification of an Active Directory replica source naming context, replication of attributes for an AD DS object, or removal of a lingering object from a replica.

The `auditpol.exe` tool enables you to configure auditing from the command line. You must use this tool to enable the auditing of the new directory service access subcategories outlined here. We discuss this tool later in this section.

NOTE

These new auditing categories also apply to auditing of Active Directory Lightweight Directory Services (AD LDS).

Use of GPOs to Configure Auditing

Group Policy enables you to configure success or failure for several types of actions. In other words, you can choose to record successful actions, failed attempts at performing these actions, or both. For example, if you are concerned about intruders who might be attempting to access your network, you can log failed logon events. You can also track successful logon events, which is useful if the intruders succeed in accessing your network.

You can use Group Policy to enable auditing at domain controllers, member servers, and client computers. Be aware that all auditing takes place only at the local computer where the events take place, and that these events are recorded on that computer's Security log. To enable auditing on all domain controllers, configure the auditing settings in the Default Domain Controllers Policy GPO; to enable auditing on other domain computers, configure the auditing settings in the Default Domain Policy GPO or in another GPO as required.

Available Auditing Categories

Windows Server 2008 enables you to audit the following types of events:

- **Account logon**—Logon or logoff by a domain user account at a domain controller. You should track both success and failure.

- **Account management**—Creation, modification, or deletion of computer, user, or group accounts. Also included are enabling and disabling of accounts and changing or resetting of passwords. You should track both success and failure.
- **Directory service access**—Access to an AD DS object as specified by the object's SACL. This category includes the four subcategories mentioned earlier in this section; enabling directory service access from the Group Policy Management Editor enables all four subcategories. Enable this category for failures. (If you record success, a large number of events will be logged.)
- **Logon events**—Logon or logoff by a user at a member server or client computer. You should track both success and failure. (Success logging can record an unauthorized access that succeeded.)
- **Object access**—Access by a user to an object such as a file, folder, or printer. You need to configure auditing in each object's SACL to track access to that object. Track success and failure to access important resources on your network.
- **Policy change**—Modification of policies, including user rights assignment, trust, and audit policies. This category is not normally needed unless unusual events are occurring.
- **Privilege use**—Use of a user right, such as changing the system time. Track failure events for this category.
- **Process tracking**—Actions performed by an application. This category is primarily for application developers and does not need to be enabled in most cases.
- **System events**—Events taking place on a computer, such as an improper shutdown or a disk with little free space remaining. Track success and failure events.

NOTE

Note the difference between Logon and Account Logon events. Logon events refer to authentication of a local user at a workstation or member server, while Account Logon events refer to the authentication of a domain user account at a domain controller.

EXAM ALERT

Know which types of actions to audit for different scenarios. For example, the exam might present a drag-and-drop interface where you must select success and failure actions to achieve a given objective.

Configuring Auditing

To configure auditing policies, access the Group Policy Management Editor focused on the desired GPO. For auditing actions on domain controllers, this will generally be the Default Domain Controllers Policy GPO. Navigate to the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy node and click this node to display the available policies in the Details pane.

To enable auditing of any of these event types, right-click it and choose Properties. On the Properties dialog box shown in Figure 7.9, select Define These Policy Settings, select Success and/or Failure as required, and then click OK. New to Windows Server 2008, the Explain tab of each policy's Properties dialog box provides more information on what the setting does.

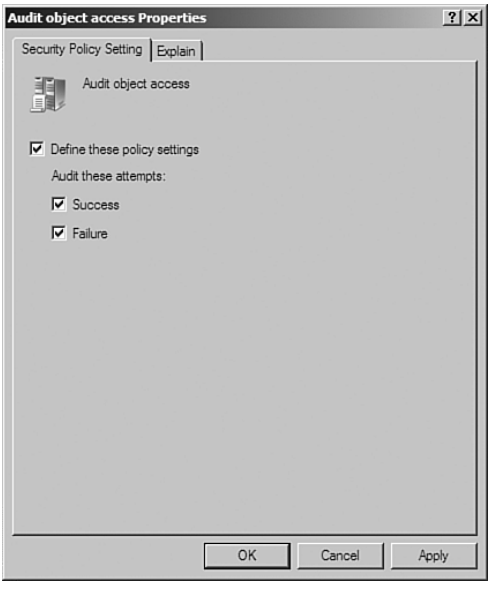

FIGURE 7.9 Enabling auditing of object access.

To track object access or directory service access, you must configure the SACL for each required object. In Windows Explorer, right-click the required file, folder, or printer, and choose Properties. On the Properties dialog box, click Advanced to open the Advanced Security Settings dialog box, and then select the Auditing tab. To add users or groups to this tab, click Edit and then click Add. Type the required users or groups in the Select User, Computer, or Group dialog box, and then click OK. On the Auditing Entry dialog box that appears (see Figure 7.10), select the types of actions you want to track, and then click OK. The completed auditing entries appear in the Advanced Security Settings dialog box, as shown in Figure 7.11. Click OK twice to close these dialog boxes.

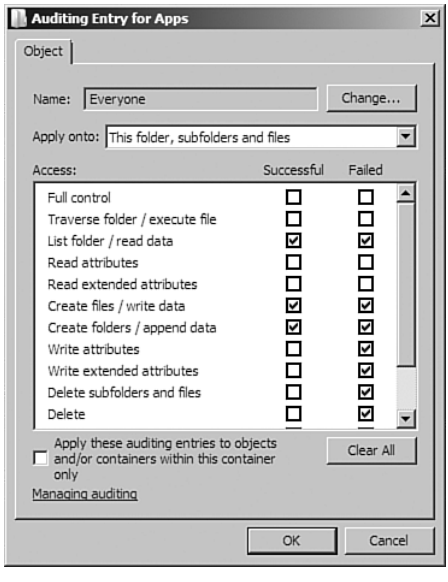

FIGURE 7.10 Configuring the SACL for an AD DS object.

After you have configured object access auditing, attempts to access audited objects appear in the Security log, which you can view from Event Viewer either in Server Manager, as shown in Figure 7.12, or in its own snap-in from the Administrative Tools folder. For more information on any audited event, right-click the event and choose Event Properties.

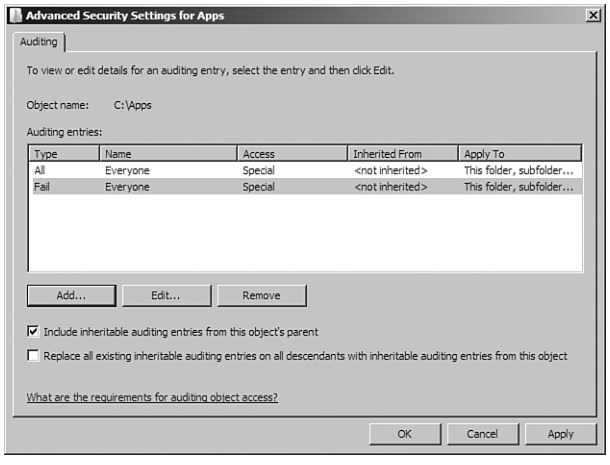

FIGURE 7.11 The Advanced Security Settings dialog box displays information on the types of object auditing actions that have been specified.

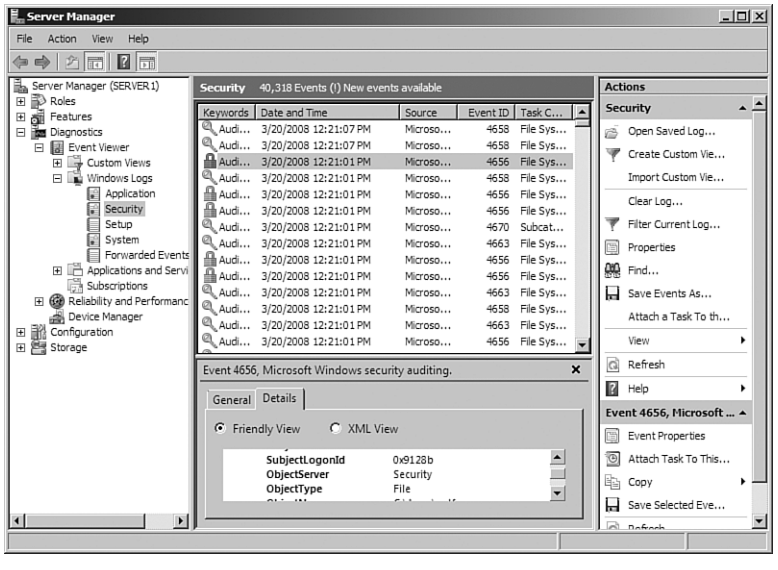

FIGURE 7.12 Event Viewer displays failed attempts at accessing an object with a lock icon.

TIP

Ensure that the Security log has adequate space to audit the events that you configure for auditing, because the log can fill rapidly. The recommended size is at least 128MB. You should also periodically save the existing log to a file and clear all past events. If the log becomes full, the oldest events are overwritten (and therefore lost) by default. You can also configure the log to archive when full and not to overwrite events, but new events are not recorded. Loss of recorded events can be serious in the case of high-security installations.

Use of `Auditpol.exe` to Configure Auditing

The `Auditpol.exe` tool performs audit policy configuration actions from the command line. This is the only tool you can use to configure auditing on a Server Core computer or to configure directory service auditing subcategories.

To use this tool, type the following at a command line:

```
Auditpol command [<sub-command><options>]
```

Table 7.1 describes the available commands, and Table 7.2 describes several of the more important subcommands and options that you should be aware of.

TABLE 7.1 `Auditpol` Commands

Command	Meaning
`/get`	Displays the current auditing policy
`/set`	Sets the audit policy
`/list`	Displays audit policy categories and subcategories, or lists users for whom a per-user audit policy is defined
`/backup`	Saves the audit policy to a specified file
`/restore`	Retrieves the audit policy from a specified file
`/clear`	Clears the audit policy
`/remove`	Removes per-user audit policy settings and disables system audit policy settings

TABLE 7.2 `Auditpol` Subcommands and Options

Option	Meaning
`/user:<username>`	Specifies the security principal for a per-user audit. Specify the username by security identifier (SID) or by name. Requires either the `/category` or `/subcategory` subcommand when used with the `/set` command.
`/category:<name>`	One or more auditing categories separated by | and specified by name or Globally Unique Identifier (GUID).
`/subcategory:<name>`	One or more auditing subcategories separated by | and specified by name or GUID.
`/success:enable`	Enables success auditing when using the `/set` command.

TABLE 7.2 *Continued*

Option	Meaning
`/success:disable`	Disables success auditing when using the `/set` command.
`/failure:enable`	Enables failure auditing when using the `/set` command.
`/failure:disable`	Disables failure auditing when using the `/set` command.
`/file`	Specifies the file to which an audit policy is to be backed up, or from which an audit policy is to be restored.

For example, to configure auditing for directory service changes, you type the following:

```
Auditpol /set /subcategory:"directory service changes" /success:enable
```

Additional subcommands and options are available with most of the `auditpol` commands discussed here. For information on the available subcommands and options available for a specified command, type **`auditpol /`*`command`*` /?`**.

Exam Cram Questions

1. Evan is responsible for configuring Group Policy in his company's domain. The domain functional level is set to Windows Server 2003. Evan's manager has requested that he implement an account policy that specifies that all user accounts will be locked out if an incorrect password is entered five times within a one-quarter hour period. The account is to remain locked out until a support technician unlocks it.

   How should Evan configure the account policy? (Each correct answer represents part of the solution. Choose three answers.)

   - ❍ **A.** Set the account lockout threshold to 0.
   - ❍ **B.** Set the account lockout threshold to 1.
   - ❍ **C.** Set the account lockout threshold to 4.
   - ❍ **D.** Set the account lockout duration to 0.
   - ❍ **E.** Set the account lockout duration to 1.
   - ❍ **F.** Set the reset account lockout counter value to 0.25.
   - ❍ **G.** Set the reset lockout counter to 15.
   - ❍ **H.** Set the reset lockout counter to 900.

2. Laura is the systems administrator for a company that operates an AD DS domain. The domain and forest functional level are set to Windows Server 2008. She has configured a password policy for users in her company's domain that specifies that passwords must be at least seven characters long. The CIO has informed her that users in the legal department should have highly secure passwords. She configures a password policy in a GPO linked to the Legal OU that specifies that passwords be at least 12 characters long.

   A few days later, she receives a call from the CIO asking her why she has not yet implemented the stricter password policy. What must Laura do to implement the policy with the least amount of administrative effort?

   - ❍ **A.** She needs to create a global security group, add the required users to this group, and ensure that the group has the Allow–Apply Group Policy permission applied to it.
   - ❍ **B.** She needs to create a new domain, place the legal users and their computers in this domain, and then reapply the password policy to this domain.
   - ❍ **C.** She needs to create a password settings object containing the required password settings and apply this object to the Legal OU.

- ❍ **D.** She needs to create a global security group and add the required users to this group. She then needs to create a password settings object containing the required password settings and apply this object to the group containing these users.

3. You are excited about the new capability of configuring fine-grained password policies and want to try it out. To which of the following groups should your user account belong so that you can configure a fine-grained password policy?

- ❍ **A.** Account Operators
- ❍ **B.** Domain Admins
- ❍ **C.** Enterprise Admins
- ❍ **D.** Schema Admins

4. Dennis is responsible for configuring security settings on a Windows Server 2008 computer. This computer runs specialized software and is configured as a standalone server that is not a member of his company's AD DS domain. He needs to configure security settings that are similar to those applied to member servers in the domain.

What should Dennis do to accomplish this task with the least amount of administrative effort?

- ❍ **A.** He should use the Security Templates snap-in to create a security database of the settings on a member server. He should then use the Security Configuration and Analysis snap-in to configure the standalone server with the settings contained in the database.
- ❍ **B.** He should use the Security Configuration and Analysis snap-in to analyze the security settings on the member server and then use this snap-in to configure the standalone server with the settings contained in the database.
- ❍ **C.** He should use the Security Templates snap-in to configure the security settings on the standalone server with settings contained in the `Securews.inf` security template.
- ❍ **D.** He should copy the settings on the member server and configure these settings manually on the standalone server.

5. You are the administrator of a company that operates an AD DS network that contains two domains. Both domains operate at the Windows Server 2003 domain and forest functional levels. You have installed a new Windows Server 2008 computer and promoted this server to be an additional domain controller in your domain.

Having heard about the new capability of configuring fine-grained password policies, you decide to give it a try and configure a PSO that specifies a minimum of 10 characters. You then associate this PSO with your user account and attempt to change your password to a new one that is 8 characters long.

When this attempt succeeds, you wonder why the new PSO was not applied to your account. Which of the following is the reason you were able to specify an 8-character password?

- ❍ **A.** You need to associate the PSO with a global security group to which your user account belongs before it is applied.
- ❍ **B.** You need to associate the PSO with an OU to which your user account belongs before it is applied.
- ❍ **C.** You need to upgrade all domain controllers in the domain to Windows Server 2008 and set the domain functional level to Windows Server 2008 before the PSO is effective.
- ❍ **D.** You need to upgrade all domain controllers in both domains of the forest to Windows Server 2008 and set the domain and forest functional levels to Windows Server 2008 before the PSO is effective.

6. Ruth is the administrator of an AD DS network that operates at the Windows Server 2008 domain and forest functional level. Her manager has asked her to implement success and failure auditing of directory service changes on the domain controller. The manager does not want success auditing of directory service access to be implemented because problems have occurred with events being overwritten in security logs before Ruth has had time to check them.

Which of the following tools should Ruth use to configure auditing as requested?

- ❍ **A.** `Auditpol.exe`
- ❍ **B.** `ADSIEdit.exe`
- ❍ **C.** `Ntdsutil.exe`
- ❍ **D.** Group Policy Management Editor

7. Barry is the network administrator for Examcram.com, which operates an AD DS network. The network includes servers running Windows Server 2003 and Windows Server 2008 and client computers running Windows XP Professional and Windows Vista Business. His manager has requested that he implement auditing of the following:

- ▶ Attempts to log on to any local computer
- ▶ Creation of a user account or group or changing of a user account password

What auditing components should Barry configure? (Each correct answer represents part of the solution. Choose two answers.)

- ❍ **A.** Audit account management, success
- ❍ **B.** Audit account logon events, success and failure
- ❍ **C.** Audit object access, success
- ❍ **D.** Audit logon events, success and failure

8. Veronica is responsible for configuring Group Policy on her company's AD DS network. She has deployed a new software package to all computers in the Financial OU. Users in this OU report that their computers are restarting spontaneously at frequent intervals.

   Veronica wants to enable an auditing policy in a GPO in an attempt to troubleshoot this problem. Which type of events should she audit?

   - ❍ **A.** Logon events
   - ❍ **B.** Process tracking events
   - ❍ **C.** System events
   - ❍ **D.** Privilege use events
   - ❍ **E.** Policy change events

Answers to *Exam Cram* Questions

1. **C, D, G.** Evan should specify an account lockout threshold of 4 passwords, and account lockout duration of 0, and a reset account lockout counter value of 15 minutes. The account lockout threshold specifies the number of incorrect passwords that can be entered before the account locks out. It can be set from 0 to 999, and a value of 0 means that the account never locks out. The account lockout duration can be set from 0 to 99,999 minutes, and a value of 0 means that the account remains locked out until unlocked by an administrator or individual who has been delegated this responsibility. The reset account lockout counter value specifies the number of minutes to wait until the lockout counter resets itself to 0. It can be set to any value between 0 and 99999; a value of 0 means that this counter is never reset. If Evan set an account lockout threshold to 0, the accounts would never lock out, and if he set it to 1, the accounts would lock out after one incorrect password, so answers A and B are incorrect. If Evan set the account lockout duration to 1, the accounts would lock out for one minute only, so answer E is incorrect. If he set the reset account lockout counter value to 0, the account lockout counter would never reset, so answer F is incorrect. If he set the reset account lockout counter to 900, the counter would not reset until 15 hours had elapsed. (The value of this counter is specified in minutes, not seconds.) Therefore, answer H is incorrect.

2. **D.** Laura needs to create a global security group and add the required users to this group. She then needs to create a password settings object containing the required

password settings and apply this object to the group containing these users. The new fine-grained password policy in Windows Server 2008 enables her to create a password policy that applies only to specified users or groups. Laura cannot link a GPO to a group, so answer A is incorrect. Laura could create a new domain and apply the policy in this manner. This was the method she would have needed to do before Windows Server 2008; however, application of a fine-grained password policy takes far less administrative effort and expense, so answer B is incorrect. It is not possible to apply a fine-grained password policy to an OU, so answer C is incorrect.

3. **B.** Your user account must belong to the Domain Admins global group before you can create a fine-grained password policy. Membership in the Account Operators group is insufficient, so answer A is incorrect. Membership in either the Enterprise Admins or Schema Admins group is not required for creating a fine-grained password policy, so answers C and D are incorrect.

4. **A.** Dennis should use the Security Templates snap-in to create a security database of the settings on a member server. He should then use the Security Configuration and Analysis snap-in to configure the standalone server with the settings contained in the database. This procedure copies the security settings that he has already configured to the standalone server; he can subsequently configure any additional settings that might be needed manually. The Security Configuration and Analysis snap-in does not create a database of settings, it compares existing settings to those in the database and configures the server to these settings; therefore, answer B is incorrect. The `Securews.inf` security template was used in Windows 2000 and Windows Server 2003 to configure security settings on member servers and workstations. It is no longer available in Windows Server 2008, so answer C is incorrect. Dennis could manually configure settings, but this would take far more administrative effort, so answer D is incorrect.

5. **C.** To have a PSO apply properly, the domain functional level must be at the Windows Server 2008 functional level. To achieve this functional level, you must upgrade all domain controllers to Windows Server 2008. You can associate a PSO with a user account, so answer A is incorrect. It is not possible to associate a PSO with an OU, so answer B is incorrect. It is not necessary to upgrade other domains in the forest to Windows Server 2008 if no PSO is being applied in these domains, so answer D is incorrect.

6. **A.** Ruth should use the `Auditpol.exe` command-line tool to configure auditing of directory service changes. This is a new auditing category that is included in the Directory Service Access category but must be configured from `Auditpol.exe` to be implemented on its own. Ruth would use `ADSIEdit.exe` to perform low-level editing of AD DS objects, including the implementation of fine-grained password policies. She would use `Ntdsutil.exe` to perform several AD DS management actions, including the seizure of operations masters roles. Neither of these tools can be used to configure auditing, so answers B and C are incorrect. Ruth could implement auditing of the Directory Service Access category from the Group Policy Management Console, but this would not fulfill the requirements of this scenario, so answer D is incorrect.

7. **A, D.** The audit account management event includes creation, modification, or deletion of user accounts or groups, renaming or disabling of user accounts, or configuring and changing of passwords; and the audit logon events tracks logons at local computers. Audit account logon events are logon and logoff activity at member servers and client computers, so answer B is incorrect. Audit object access tracks when a user accesses an object such as a file, folder, Registry key, or printer that has its own SACL specified, so answer C is incorrect.

8. **C.** Veronica should implement success auditing of system events to identify the cause of the problems that are being experienced. This tracks actions taking place on a computer, such as improper shutdowns or restarts. Logon events track logon and logoff activity at member servers and client computers, but they do not track the causes of improper shutdowns as experienced here, so answer A is incorrect. Process tracking events track actions performed by an application, but not improper shutdowns, so answer B is incorrect. Privilege use events track the use of system rights, so answer D is incorrect. Policy change events track the modification of policies including user rights assignment, trust, and audit policies. This also is not required here, so answer E is incorrect.

Index

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

R

S

T

U

V

W

X-Y-Z

zones