DON POULTON

Cert Guide

Learn, prepare, and practice for exam success

- Master every topic on Microsoft's new MCTS 70-640 exam.
- Assess your knowledge and focus your learning.
- Get the practical workplace knowledge you need!

MCTS 70-640

Windows Server 2008 Active Directory, Configuring

CD INCLUDES COMPLETE SAMPLE EXAM

PEARSON

MCTS 70-640 Cert Guide: Windows Server 2008 Active Directory, Configuring

Don Poulton

Pearson
800 East 96th Street
Indianapolis, Indiana 46240 USA

MCTS 70-640 Cert Guide: Windows Server 2008 Active Directory, Configuring

ISBN-13: 978-0-7897-4708-2
ISBN-10: 0-7897-4708-1
Library of Congress Cataloging-in-Publication Data:
Poulton, Don.
MCTS 70-640 cert guide : Windows server 2008 Active directory, configuring / Don Poulton.
p. cm.
ISBN 978-0-7897-4708-2 (hardcover w/CD)
1. Microsoft Windows server--Examinations--Study guides. 2. Operating systems (Computers)--Examinations--Study guides. 3. Directory services (Computer network technology)--Examinations--Study guides. 4. Local area networks (Computer networks)--Management--Examinations--Study guides. 5. Telecommunications engineers--Certification. 6. Electronic data processing personnel--Certification. I. Title. II. Title: Windows server 2008 Active directory, configuring.
QA76.76.O63P6685 2011
005.4'476--dc22
2010043593
Printed in the United States of America
First Printing: December 2010

Bulk Sales

Que Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales international@pearson.com

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Box Twelve Communications, Inc.

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Mike Henry

Indexer
Erika Millen

Proofreader
Megan Wade

Technical Editor
Chris Crayton

Publishing Coordinator
Vanessa Evans

Multimedia Developer
Dan Scherf

Designer
Gary Adair

Page Layout
Mark Shirar

Contents at a Glance

Table of Contents

About the Author

Don Poulton (A+, Network+, Security+, MCSA, MCSE) is an independent consultant who has been involved with computers since the days of 80-column punch cards. After a career of more than 20 years in environmental science, Don switched careers and trained as a Windows NT 4.0 MCSE. He has been involved in consulting with a couple of small training providers as a technical writer, during which time he wrote training and exam prep materials for Windows NT 4.0, Windows 2000, and Windows XP. Don has written or contributed to several titles, including *Security+ Lab Manual* (Que, 2004); *MCSA/MCSE 70-299 Exam Cram 2: Implementing and Administering Security in a Windows 2003 Network (Exam Cram 2)* (Que, 2004); *MCSE 70-294 Exam Prep: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure* (Que, 2006); *MCTS 70-620 Exam Prep: Microsoft Windows Vista, Configuring* (Que, 2008); and *MCTS 70-680 Cert Guide: Microsoft Windows 7, Configuring* (Que, 2011).

In addition, he has worked on programming projects, both in his days as an environmental scientist and more recently with Visual Basic to update an older statistical package used for multivariate analysis of sediment contaminants.

When not working on computers, Don is an avid amateur photographer who has had his photos displayed in international competitions and published in magazines such as *Michigan Natural Resources Magazine* and *National Geographic Traveler*. Don also enjoys traveling and keeping fit.

Don lives in Burlington, Ontario, with his wife, Terry.

Dedication

I would like to dedicate this book to my wife Terry, who has stood by my side and supported me throughout the days spent writing this book. This project would not have been possible without her love and support.

Acknowledgments

I would like to thank all the staff at Pearson and in particular Betsy Brown for making this project possible. My sincere thanks goes out to Chris Crayton for his helpful technical suggestions, as well as Jeff Riley, development editor, and Mike Henry, copy editor, for their improvements to the manuscript.

—Don Poulton

About the Technical Reviewer

Christopher A. Crayton is an author, technical editor, technical consultant, security consultant, trainer, and SkillsUSA state-level technology competition judge. Formerly, he worked as a computer and networking instructor at Keiser College (2001 Teacher of the Year); as network administrator for Protocol, a global electronic customer relationship management (eCRM) company; and at Eastman Kodak Headquarters as a computer and network specialist. Chris has authored several print and online books, including The *A+ Exams Guide*, *Second Edition* (Cengage Learning, 2008); *Microsoft Windows Vista 70-620 Exam Guide Short Cut* (O'Reilly, 2007); *CompTIA A+ Essentials 220-601 Exam Guide Short Cut* (O'Reilly, 2007); *The A+ Exams Guide* (Charles River Media, 2008); *The A+ Certification and PC Repair Handbook* (Charles River Media, 2005); *The Security+ Exam Guide* (Charles River Media, 2003); and *A+ Adaptive Exams* (Charles River Media, 2002). He is also coauthor of the *How to Cheat at Securing Your Network* (Syngress, 2007). As an experienced technical editor, Chris has provided many technical edits/reviews for several major publishing companies, including Pearson Education, McGraw-Hill, Cengage Learning, Wiley, O'Reilly, Syngress, and Apress. He holds MCSE, A+, and Network+ certifications.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As an associate publisher for Pearson Publishing, I welcome your comments. You can email or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

When you write, please be sure to include this book's title and author as well as your name, email address, and phone number. I will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Dave Dusthimer
Associate Publisher
Pearson Education
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonITcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

MCTS Windows Server 2008 Active Directory, Configuring Cert Guide (Exam 70-640) is designed for network administrators, network engineers, and consultants who are pursuing the Microsoft Certified Technology Specialist (MCTS) or Microsoft Certified IT Professional (MCITP) certifications for Windows Server 2008. This book covers the "TS: Microsoft Windows Server 2008 Active Directory, Configuring" exam (70-640), which earns you the Microsoft Certified Technology Specialist: Windows Server 2008 Active Directory, Configuration certification. The exam is designed to measure your skill and ability to implement, administer, and troubleshoot Active Directory running on Windows Server 2008. Microsoft not only tests you on your knowledge of Active Directory, but it has purposefully developed questions on the exam to force you to problem-solve in the same way that you would when presented with a real-life error. Passing this exam demonstrates your competency in administration.

This book covers all the objectives that Microsoft has established for exam 70-640. It doesn't offer end-to-end coverage of Active Directory in Windows Server 2008; rather, it helps you develop the specific core competencies that you need to master as an Active Directory administrator. You should be able to pass the exam by learning the material in this book, without taking a class.

Goals and Methods

The number-one goal of this book is a simple one: to help you get ready to take—and pass—Microsoft Certification Exam 70-640, "TS: Windows Server 2008 Active Directory, Configuring." You will find information within this book that will help ensure your success as you pursue this Microsoft exam and the Technology Specialist or IT Professional certification.

Because Microsoft certification exams stress problem-solving abilities and reasoning more than memorization of terms and facts, our goal is to help you master and understand the required objectives for the 70-640 exam.

To aid you in mastering and understanding the MCTS certification objectives, this book uses the following methods:

- **Opening topics list:** This defines the topics to be covered in the chapter; it also lists the corresponding 70-640 exam objectives.
- **Do I Know This Already Quizzes:** At the beginning of each chapter is a quiz. The quizzes, and answers/explanations (found in Appendix A), are meant to gauge your knowledge of the subjects. If the answers to the questions don't come readily to you, be sure to read the entire chapter.
- **Foundation Topics:** The heart of the chapter. Explains the topics from a hands-on and a theory-based standpoint. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. The chapters are broken down into several topics each.
- **Key Topics:** The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table form at the end of the chapter.
- **Memory Tables:** These can be found on the DVD within Appendix C, "Memory Tables." Use them to help memorize important information.
- **Key Terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the complete key terms in the glossary.

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and enable you to easily move between chapters and sections of chapters to cover just the material that you need more work with. If you do intend to read all the chapters, the order in the book is an excellent sequence to use.

Chapter 1, "Getting Started with Active Directory," is an introductory chapter that presents the concepts around which Active Directory is built. It serves as a reference to the material that follows and eases users who are new to Active Directory into the book. If you have worked with Active Directory in Windows 2000 or Windows Server 2003, you might want to start with Chapter 2; however, you should take a look at the overview presented here of new capabilities of Active Directory in Windows Server 2008 and its R2 update.

The core chapters, Chapters 2 through 17, cover the following topics:

- **Chapter 2, "Installing and Configuring DNS for Active Directory":** This chapter focuses on the concepts of Domain Name System (DNS) required for setting up an Active Directory domain. You learn about how to install DNS on your server and how to set up and configure DNS zones.
- **Chapter 3, "Installing Active Directory Domain Services":** This chapter shows you how to set up your first domain. It then continues to discuss creating additional domain controllers in this domain and child domain controllers. It also discusses the requirements that must be met when upgrading domains based on older Windows server versions to allow them to operate in Windows Server 2008 with complete functionality.
- **Chapter 4, "Configuring DNS Server Settings and Replication":** This chapter builds on Chapter 2 to delve into additional items that you must configure in server settings, zone transfers, and DNS replication.
- **Chapter 5, "Global Catalogs and Operations Masters":** Proper operation of global catalog servers and operations masters is vital to the day-to-day functioning of your domain and forest. This chapter focuses on the configuration and troubleshooting steps necessary with these specialized domain controllers.
- **Chapter 6, "Configuring Active Directory Sites and Replication":** Active Directory divides forests and domains on a geographical basis by using sites. To function properly, Active Directory depends on data replication among all its domain controllers. This chapter shows you how to set up sites and ensure that all directory objects are located in the site corresponding to their locations. It then continues with configuring replication, both on an intrasite and intersite basis.
- **Chapter 7, "Additional Active Directory Roles":** This chapter takes care of other Active Directory roles including Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS), and Active Directory Rights Management Service (AD RMS). AD LDS is designed to provide additional directory services where an additional domain and its domain controllers are not required. AD RMS enhances security in your domain by enabling the creation of rights-protected files and folders that can be accessed only by authorized users. AD FS provides a single sign-on capability for authenticating users to multiple web-based applications.
- **Chapter 8, "Read-Only Domain Controllers":** This chapter discusses how to set up a read-only domain controller (RODC) and configure its interaction with

other (writable) domain controllers in your forest. An RODC is useful in a situation such as a branch office where physical security of the domain controller might be of concern.

- **Chapter 9, "Active Directory User and Group Accounts":** This chapter shows you how to create user and group accounts in Active Directory, including methods for bulk creation of large numbers of accounts. It introduces the various types and scopes of groups available in Active Directory and the recommended methods of nesting these groups to facilitate the provision of access to resources in your forest. It also looks at account properties, creation of organizational units (OUs), and delegation of control.
- **Chapter 10, "Trust Relationships in Active Directory":** By default, all domains in a forest trust each other. However, you might need to access objects located in another forest, and this chapter talks about methods you might use to provide and troubleshoot such access. Windows Server 2008 provides several types of trust relationships that can be used for meeting different requirements.
- **Chapter 11, "Creating and Applying Group Policy Objects":** Group Policy is at the heart and soul of resource management in Active Directory. This chapter shows you how to set up Group Policy objects and configure them to apply to users, groups, and OUs as required. The hierarchy of GPO application and the methods to modify this hierarchy are also discussed.
- **Chapter 12, "Group Policy Software Deployment":** This chapter shows you how to use Group Policy for deploying software to large numbers of users so that they have the applications they need to perform their jobs. You also learn how to upgrade software when new editions and features become available and how to remove software when it is no longer required by users.
- **Chapter 13, "Account Policies and Audit Policies":** This chapter expands the coverage of Group Policy to include policies that govern the safety and security of accounts in your domain and audit access to Active Directory objects and components so that you can meet the increasingly complex regulatory requirements.
- **Chapter 14, "Monitoring Active Directory":** This chapter focuses on the tools you can use to monitor the functionality of Active Directory. You also learn about the tools and methods used for monitoring Active Directory replication as well as the tools and techniques you can use to monitor and troubleshoot the application of Group Policy.
- **Chapter 15, "Maintaining Active Directory":** This chapter shows you how to back up, recover, restart, and troubleshoot Active Directory and its components.

You learn how to perform nonauthoritative and authoritative restore of Active Directory and how to use the new Windows Server 2008 R2 Active Directory Recycle Bin.

- **Chapter 16, "Installing and Configuring Certificate Services":** A system of certificates is vital to carrying out secure business, especially when an Internet presence is required. This chapter shows you how to set up a hierarchy of certificate servers within Active Directory and back up, restore, and archive your certificates and keys.
- **Chapter 17, "Managing Certificate Templates, Enrollments, and Certificate Revocation":** Certificates issued by your servers require management to ensure that users requiring certificates can obtain them, and that compromised certificates are revoked and cannot be used by unauthorized parties. This chapter looks at these topics and helps you to ensure the security of your certificate hierarchy.

In addition to the 17 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The CD includes the glossary, practice test, and memory tables that you can work through to verify your knowledge of the subject matter.

Study and Exam Preparation Tips

It's a rush of adrenaline during the final day before an exam. If you've scheduled the exam on a workday, or following a workday, you will find yourself cursing the tasks you normally cheerfully perform because the back of your mind is telling you to read just a bit more, study another scenario, practice another skill so that you will be able to get this exam out of the way successfully.

The way that Microsoft has designed its tests lately does not help. I remember taking Microsoft exams many years ago and thoroughly understanding the term *paper certified*. Nowadays, you can't get through a Microsoft exam without knowing the material so well that when confronted with a problem, whether a scenario or real-life situation, you can handle the challenge. Instead of trying to show the world how many MCSEs are out there, Microsoft is trying to prove how difficult it is to achieve a certification, including the newly created MCTS and MCITP as well as the MCSE and MCSA, thereby making those who are certified more valuable to their organizations.

Learning Styles

To best understand the nature of preparation for the test, it is important to understand learning as a process. You are probably aware of how you best learn new

material. You might find that outlining works best for you, or, as a visual learner, you might need to "see" things. Or, as a person who studies kinesthetically, the hands-on approach serves you best. Whether you need models or examples, or you just like exploring the interface, or whatever your learning style, solid test preparation works best when it takes place over time. Obviously, you shouldn't start studying for a certification exam the night before you take it; it is very important to understand that learning is a developmental process. Understanding learning as a process helps you focus on what you know and what you have yet to learn.

People study in a combination of different ways: by doing, by seeing, and by hearing and writing. This book's design fulfills all three of these study methods. For the kinesthetic, there are key topics scattered throughout each chapter. You will also discover step-by-step procedural instructions that walk you through the skills you need to master Active Directory in Windows Server 2008. The visual learner can find plenty of screen shots explaining the concepts described in the text. The auditory learner can reinforce skills by reading out loud and copying down key concepts and exam tips scattered throughout the book. You can also practice writing down the meaning of the key terms defined in each chapter, and in completing the memory tables for most chapters found on the accompanying DVD. While reading this book, you will realize that it stands the test of time. You will be able to turn to it over and over again.

Thinking about how you learn should help you recognize that learning takes place when you are able to match new information to old. You have some previous experience with computers and networking. Now you are preparing for this certification exam. Using this book, software, and supplementary materials will not just add incrementally to what you know; as you study, the organization of your knowledge actually restructures as you integrate new information into your existing knowledge base. This leads you to a more comprehensive understanding of the tasks and concepts outlined in the objectives and of computing in general. Again, this happens as a result of a repetitive process rather than a singular event. If you keep this model of learning in mind as you prepare for the exam, you will make better decisions concerning what to study and how much more studying you need to do.

Study Tips

There are many ways to approach studying, just as there are many different types of material to study. However, the tips that follow should work well for the type of material covered on Microsoft certification exams.

Study Strategies

Although individuals vary in the ways they learn information, some basic principles of learning apply to everyone. You should adopt some study strategies that take advantage of these principles. One of these principles is that learning can be broken into various depths. Recognition (of terms, for example) exemplifies a rather surface level of learning in which you rely on a prompt of some sort to elicit recall. Comprehension or understanding (of the concepts behind the terms, for example) represents a deeper level of learning than recognition. The ability to analyze a concept and apply your understanding of it in a new way represents further depth of learning.

Your learning strategy should enable you to know the material at a level or two deeper than mere recognition. This will help you perform well on the exams. You will know the material so thoroughly that you can go beyond the recognition-level types of questions commonly used in fact-based multiple-choice testing. You will be able to apply your knowledge to solve new problems.

Macro and Micro Study Strategies

One strategy that can lead to deep learning includes preparing an outline that covers all the objectives and subobjectives for the particular exam you are planning to take. You should delve a bit further into the material and include a level or two of detail beyond the stated objectives and subobjectives for the exam. Then you should expand the outline by coming up with a statement of definition or a summary for each point in the outline.

An outline provides two approaches to studying. First, you can study the outline by focusing on the organization of the material. You can work your way through the points and subpoints of your outline, with the goal of learning how they relate to one another. For example, you should be sure you understand how each of the main objective areas for Exam 70-640 is similar to and different from another. Then you should do the same thing with the subobjectives; you should be sure you know which subobjectives pertain to each objective area and how they relate to one another.

Next, you can work through the outline, focusing on learning the details. You should memorize and understand terms and their definitions, facts, rules and tactics, advantages and disadvantages, and so on. In this pass through the outline, you should attempt to learn detail rather than the big picture (the organizational information that you worked on in the first pass through the outline).

Research has shown that attempting to assimilate both types of information at the same time interferes with the overall learning process. If you separate your studying into these two approaches, you will perform better on the exam.

Active Study Strategies

The process of writing down and defining objectives, subobjectives, terms, facts, and definitions promotes a more active learning strategy than merely reading the material does. In human information-processing terms, writing forces you to engage in more active encoding of the information. Simply reading over the information leads to more passive processing. Using this study strategy, you should focus on writing down the items that are highlighted in the book—bulleted or numbered lists, key topics, notes, cautions, and review sections, for example.

You need to determine whether you can apply the information you have learned by attempting to create examples and scenarios on your own. You should think about how or where you could apply the concepts you are learning. Again, you should write down this information to process the facts and concepts in an active fashion.

Common-Sense Strategies

You should follow common-sense practices when studying: You should study when you are alert, reduce or eliminate distractions, and take breaks when you become fatigued.

Pretesting Yourself

Pretesting allows you to assess how well you are learning. One of the most important aspects of learning is what has been called *meta-learning*. Meta-learning has to do with realizing when you know something well or when you need to study some more. In other words, you recognize how well or how poorly you have learned the material you are studying.

For most people, this can be difficult to assess. Memory tables, practice questions, and practice tests are useful in that they reveal objectively what you have learned and what you have not learned. You should use this information to guide review and further studying. Developmental learning takes place as you cycle through studying, assessing how well you have learned, reviewing, and assessing again until you feel you are ready to take the exam.

You might have noticed the practice exam included in this book. You should use it as part of the learning process. The Exam Gear test-simulation software included on this book's CD-ROM also provides you with an excellent opportunity to assess your knowledge.

You should set a goal for your pretesting. A reasonable goal would be to score consistently in the 90% range.

Exam Prep Tips

After you have mastered the subject matter, the final preparatory step is to understand how the exam will be presented. Make no mistake: An MCTS exam challenges

both your knowledge and your test-taking skills. Preparing for the 70-640 exam is a bit different from preparing for those old Microsoft exams. The following is a list of things that you should consider doing:

- **Combine your skill sets into solutions:** In the past, exams would test whether you knew to select the right letter of a multiple choice answer. Today, you need to know how to resolve a problem that may involve different aspects of the material covered. For example, on exam 70-640 you could be presented with a problem that requires you to understand how to configure Group Policy to apply to a specific set of users and not to other users, and to troubleshoot this policy if it is not properly applied. The skills themselves are simple. Being able to zero in on what caused the problem and then to resolve it for a specific situation is what you need to demonstrate. In fact, you should not only be able to select one answer, but also multiple parts of a total solution.
- **Delve into excruciating details:** The exam questions incorporate a great deal of information in the scenarios. Some of the information is ancillary: It will help you rule out possible issues, but not necessarily resolve the answer. Some of the information simply provides you with a greater picture, as you would have in real life. Some information is key to your solution. For example, you might be presented with a question that lists the components of an Active Directory domain such as the number of server and client computers, the organizational unit (OU) structure, and so on. When you delve further into the question, you realize that the OU structure is the problem. Other times, you will find that the OU structure simply eliminates one or more of the answers that you could select. If you don't pay attention to what you can eliminate, the answer can elude you completely. And other times, the hardware configuration simply lets you know that the hardware is adequate.
- **Microsoft likes to quiz exam takers on the latest modifications of its technology:** From time to time, Microsoft seeds new questions into its exam database and beta tests these questions on exam takers. During the beta period for each question, its answer is not taken into account in computing the final score. However, when Microsoft is satisfied with the question's performance, it becomes live and is scored appropriately. You can expect to see questions that test your knowledge of the latest changes in Active Directory technology, including the enhancements introduced in 2009 with Windows Server 2008 R2.
- **It's a GUI test:** Microsoft has expanded its testing criteria into interface recognition. You should be able to recognize each dialog box, properties sheet, options, and defaults. You will be tested on how to perform typical configuration actions in Active Directory. In fact, Microsoft has begun to include performance-based questions on its exams that instruct you to perform a given task and presents

you with a live version of some Active Directory tool. You must complete the required actions and no others; otherwise, your response will be scored as incorrect.

- **Practice with a time limit:** The tests have always been time restricted, but it takes more time to read and understand the scenarios now and time is a whole lot tighter. To get used to the time limits, test yourself with a timer. Know how long it takes you to read scenarios and select answers.

Microsoft 70-640 Exam Topics

Table I-1 lists the exam topics for the Microsoft 70-640 exam. This table also lists the book parts in which each exam topic is covered.

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
1	The Foundation of Active Directory The Building Blocks of Active Directory New Features of Active Directory in Windows Server 2008	(n/a)
2	The Hierarchical Nature of DNS Installing DNS on Windows Server 2008 Configuring DNS Zones	Configuring Domain Name System (DNS) for Active Directory ■ Configure Zones
3	Planning the Active Directory Namespace Creating Forests and Domains Upgrading Older Versions of Active Directory Additional Forest and Domain Configuration Tasks	Configuring the Active Directory Infrastructure ■ Configure a forest or a domain
4	Configuring DNS Server Settings Configuring Zone Transfers and Replication	Configuring Domain Name System (DNS) for Active Directory ■ Configure DNS Server Settings ■ Configure DNS Zone Transfers and Replication

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
5	Configuring Global Catalog Servers Configuring Operations Masters	Configuring the Active Directory Infrastructure ■ Configure the global catalog ■ Configure operations masters
6	The Need for Active Directory Sites Configuring Sites and Subnets Site Links, Site Link Bridges, and Bridgehead Servers Configuring Active Directory Replication	Configuring the Active Directory Infrastructure ■ Configure sites ■ Configure Active Directory replication
7	New Server Roles and Features Active Directory Lightweight Directory Services (AD LDS) Active Directory Rights Management Services (AD RMS) Active Directory Federation Services (AD FS) Windows Server 2008 R2 Virtualization	Configuring Additional Active Directory Server Roles ■ Configure Active Directory Lightweight Directory Services (AD LDS) ■ Configure Active Directory Rights Management Service (AD RMS) ■ Configure Active Directory Federation Services (AD FS)
8	Installing a Read-Only Domain Controller Managing a Read-Only Domain Controller	Configuring Additional Active Directory Server Roles ■ Configure the read-only domain controller (RODC)
9	Creating User and Group Accounts Managing and Maintaining Accounts	Creating and Maintaining Active Directory Objects ■ Automate creation of Active Directory accounts ■ Maintain Active Directory accounts
10	Types of Trust Relationships Creating and Configuring Trust Relationships Managing Trust Relationships	Configuring the Active Directory Infrastructure ■ Configure trusts

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
11	Overview of Group Policy Creating and Applying GPOs Configuring GPO Templates	Creating and Maintaining Active Directory Objects ■ Create and apply Group Policy objects (GPOs) ■ Configure GPO templates
12	Types of Software Deployment Deploying Software Using Group Policy Upgrading Software Removal of Software	Creating and Maintaining Active Directory Objects ■ Configure software deployment GPOs
13	Use of Group Policy to Configure Security Auditing of Active Directory Services	Creating and Maintaining Active Directory Objects ■ Configure account policies ■ Configure audit policy by using GPOs
14	Tools Used to Monitor Active Directory Monitoring and Troubleshooting Active Directory Replication Troubleshooting the Application of Group Policy Objects	Maintaining the Active Directory Environment ■ Monitor Active Directory
15	Backing Up and Recovering Active Directory Offline Maintenance of Active Directory	Maintaining the Active Directory Environment ■ Configure backup and recovery ■ Perform offline maintenance
16	What's New with Certificate Services in Windows Server 2008? Installing Active Directory Certificate Services Configuring Certificate Authority Server Settings	Configuring Active Directory Certificate Services ■ Install Active Directory Certificate Services ■ Configure CA server settings

Table I-1 Microsoft 70-640 Exam Topics

Chapter	Topics	70-640 Exam Objectives Covered
17	Managing Certificate Templates Managing Certificate Enrollments Managing Certificate Revocation	Configuring Active Directory Certificate Services ■ Manage certificate templates ■ Manage enrollments ■ Manage certificate revocation

This chapter covers the following subjects:

- **Planning the Active Directory Namespace:** This section provides a basic introduction to best practices you should follow in planning and designing an Active Directory namespace that will serve your company properly both now and in the years to come.
- **Creating Forests and Domains:** In this section, you learn how to create your first domain controller in a new Active Directory forest. You then learn how to add additional domain controllers to your forest and create child domains.
- **Interoperability with Previous Versions of Active Directory:** Many organizations are using Active Directory domains based on Windows 2000 and Windows Server 2003. This section takes you through the preparatory tasks you must perform before you can add a Windows Server 2008 R2 domain controller as well as the actual upgrading of older domain controllers. In addition, it introduces you to the concept of forest and domain functional levels, as well as the benefits of the newest Windows Server 2008 R2 functional levels.
- **Additional Forest and Domain Configuration Tasks:** After you have installed and configured your first domain, you should perform several additional tasks. This section discusses verifying your Active Directory installation, using the Active Directory Migration tool (ADMT), and creating alternative user principal name (UPN) suffixes.

Installing Active Directory Domain Services

In Chapter 1, "Getting Started with Active Directory," you were introduced to the basic building blocks of the logical Active Directory structure: forests, trees, domain, and organizational units (OUs). You were also introduced to the concept of sites for distinguishing portions of the network separated physically by slow WAN links. Now you begin to create an actual Active Directory forest and domain structure.

The act of installing Active Directory on a server is conceptually very simple. You need only run the Active Directory Domain Services (AD DS) Installation Wizard from the Add Roles Wizard of Server Manager and provide answers to the questions the wizard asks. The actual act of installing AD DS, however, can be thought of as the tip of the iceberg. Before you install AD DS, you need to plan how Active Directory will fit into your company's corporate and geographical structure as well as your expectations for future growth and the potential for acquiring other companies. This chapter serves only as a basic introduction to the topic of planning.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter or simply jump to the "Exam Preparation Tasks" section for review. If you are in doubt, read the entire chapter. Table 3-1 outlines the major headings in this chapter and the corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes."

Table 3-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions Covered in This Section
Planning the Active Directory Namespace	1
Creating Forests and Domains	2–7
Interoperability with Previous Versions of Active Directory	8–9
Additional Forest and Domain Configuration Tasks	10–11

1. Which of the following are best practices that you should follow when planning an AD DS domain structure? (Choose all that apply.)
   a. Employ a test lab
   b. Prepare thorough documentation
   c. Keep everyone, including top managers, informed
   d. Understand thoroughly the network's TCP/IP infrastructure
   e. Develop and adhere to an adequate security policy
   f. Know the capabilities of your WAN links

2. On which of the following editions of Windows Server 2008 R2 can you install the AD DS role? (Choose all that apply.)
   a. Web
   b. Foundation
   c. Standard
   d. Enterprise
   e. Datacenter

3. Which of the following tools can you use to install AD DS on a server running Windows Server 2008 R2? (Choose two.)
   a. The `dcpromo.exe` command
   b. The Manage Your Server tool
   c. The Configure Your Server tool
   d. The Add Roles Wizard
   e. The Add Features Wizard

4. Which of the following conditions would represent a problem when you are attempting to install the first domain controller in your domain?
   a. A DHCP server is not present.
   b. A DNS server is not present.
   c. The server's hard disk is formatted with the FAT32 file system.
   d. The server's hard disk has only 10 GB free space available.

5. Which of the following is a new AD DS administrative tool included with Windows Server 2008 R2 and was not present in older versions of Windows Server?
   a. Active Directory Users and Computers
   b. Active Directory Administrative Center
   c. Active Directory Sites and Services

d. Active Directory Domains and Trusts

e. User Manager for Domains

6. Your computer is running the Server Core edition of Windows Server 2008 R2. You want to promote this server to domain controller. What should you do?

a. Use Server Manager to run the Add Roles Wizard.

b. Use the Initial Configuration Tasks window to run the Add Roles Wizard.

c. Use `dcpromo.exe` and specify the required parameters when prompted.

d. Use `dcpromo.exe` together with an answer file that provides the required parameters.

e. You cannot promote this server to domain controller without reinstalling Windows Server 2008 as a full edition server.

7. You are the administrator of DC1, which is a Windows Server 2008 R2 domain controller in your company's domain. You are experiencing problems with DC1 and decide to run the Active Directory Installation Wizard again on this machine. What happens?

a. A new copy of the AD DS software is installed.

b. Two copies of the AD DS software will exist side-by-side.

c. The domain controller is demoted to a member server.

d. You receive an error message informing you that the wizard cannot be run again.

8. Which of the following is not a valid domain or forest functional level for a domain controller running Windows Server 2008 R2?

a. Windows 2000 mixed

b. Windows 2000 native

c. Windows Server 2003 native

d. Windows Server 2008 native

e. Windows Server 2008 R2 native

9. You have installed Windows Server 2008 R2 on a brand-new server and want to promote this server to domain controller in your domain, which has domain controllers running Windows Server 2003 and operates at the Windows Server 2003 native domain functional level. What should you do first?

a. Run `adprep /forestprep` and then run `adprep /domainprep`.

b. Run `adprep /domainprep` and then run `adprep /forestprep`.

c. Raise the domain functional level to Windows Server 2008 R2.

d. Raise the forest functional level to Windows Server 2008 R2.

10. Your company has acquired another company, and both companies operate an AD DS forest with a single domain. The CIO has decided that all users of the acquired company are to be moved into your company's domain so that the other company's forest and domain can be decommissioned. What tool should you use to assist you in this action?
    a. Active Directory Users and Computers
    b. Active Directory Administrative Center
    c. Active Directory Migration Tool (ADMT)
    d. User State Migration Tool (USMT)

11. You are the administrator for the `sales.que.com` domain. You are configuring an implicit user principal name (UPN) suffix user named Sharon. Which of the following is a valid implicit UPN?
    a. `Sharon@sales.que.com`
    b. `Sharon@sales`
    c. `Sales.que.com\Sharon`
    d. `Sales\Sharon`

Foundation Topics

Planning the Active Directory Namespace

As discussed in Chapter 1, "Getting Started with Active Directory," the domain is the primary administrative unit within an Active Directory namespace. Windows Server 2008 uses the concept of domains to separate available resources among registered users. It is also the basic security unit, as you will see throughout this book, because many of the security requirements in Active Directory are focused at the domain level. Therefore, it is important to begin the process of planning any company's Active Directory Domain Services (AD DS) namespace from the viewpoint of the domain structure.

All planning starts from the name of your company's root domain. Recall in Chapter 1 that each tree has a root domain that is located at the top of the inverted tree structure. All subdomains contain this root domain name in their own domain names. In addition, the first domain in the entire forest is not only a root domain, it is also the forest root. Also, the top-level domain names used on the Internet and defined in the DNS hierarchy are included. The latter is not an absolute requirement if you are planning a domain that has no Internet representation whatsoever, but what company these days does not have a presence on the Internet?

Therefore, it makes sense that your root domain can take the same name as your Internet domain name as registered with InterNIC (Internet Network Information Center). Consider a fictional company with an Internet domain name of `mycompany.biz`. Although you can use this name as your AD DS root domain name, it creates a risk of revealing your company's AD DS structure to the public Internet. Consequently, you might want to keep the internal name separate and use something like `mycompany.local` for the AD DS root domain name of the same fictional company.

Subdividing the Active Directory Namespace

You can subdivide your namespace within Active Directory in two ways:

- Separate domains
- Organizational units (OUs)

In many instances, the use of separate domains or OUs would serve just as well as the other. In larger companies, the use of separate domains often arose from the limitations of the Security Accounts Manager (SAM) database in Windows NT. Because the AD DS database can hold millions of objects, this limitation is seldom of importance in AD DS design. For this reason, and because a single domain structure is the easiest type of structure to administer, this method is the best means of organizing your company's namespace if possible. There is no specific need to create separate domains for administrative functions, geographical sites, or departments in the

company. Logically, you can handle this function by setting up a system of OUs. An internal system of OUs provides the following additional advantages:

- It can be administered either centrally or locally. The concept of delegation of control in AD DS facilitates the assignment of individuals as local administrators.
- User authentication is simpler and faster within a single domain environment, regardless of where a user is located.
- It is far simpler to modify when needed—for example, if your company is reorganized.
- It is flexible and can include an internal hierarchy of departments, sections, work units, and so on.

There are, however, reasons for using separate domains for discrete divisions of your company:

- This approach can facilitate decentralized administration of network resources.
- In the case of multiple Internet domain names, the domain can be built to mirror the Internet functionality.
- Multiple domains representing different geographical locations might reduce the amount of replication traffic across low wide area network (WAN) links.
- User account requirements that vary among departments or locations, such as password complexity, are more easily handled with separate domains.
- International legal and language needs might be handled more easily by using separate domains.
- Very massive organizations can be broken down into a domain structure.

Administrative or Geographical Organization of Domains

You can organize a series of domains along either administrative or geographical means. For example, Figure 3-1 shows `mycompany.biz` organized along three administrative divisions—Accounting, Products, and Advertising—all reporting to a Management group, contrasted with the company's main offices located in San Francisco, Dallas, Toronto, and Atlanta.

You need to take into account conditions that favor either the administrative or geographical model. This can include the following factors:

- Plans for future offices in additional cities
- Projected growth of each of the company's divisions
- Potential for reorganization of the company along new departmental lines
- Requirements for centralized or decentralized administration of the company

Figure 3-1 Administrative and geographical divisions of **`mycompany.biz`**.

- Needs for different security levels in either certain departments or certain offices
- Current or future use of one or more Internet DNS namespaces

Such factors suggest the best domain organization for your company's AD DS namespace.

Use of Multiple Trees

Within the AD DS forest, you can have one or more trees. As outlined in Chapter 1, the main difference between trees and forests is that domains within a tree share a contiguous namespace, whereas domains located in different trees in the same forest have a disjointed namespace. Thus, `que.com` and `examcram.com` are root domains in two separate trees of the same forest.

In almost all multiple domain enterprises, it makes sense to employ a single tree. The major exception occurs when two companies merge and want to maintain their separate identities. Their identities, and indeed their Internet namespaces, are best served by having more than one tree in the forest.

NOTE Another way of designing a multidomain forest is to employ an empty forest root domain with a series of child domains representing administrative or geographical divisions of the company. The root domain contains only a small number of objects, and you can readily control membership in the Enterprise Admins and Schema Admins groups. The impact of business decisions, such as the spin-off or

renaming of subsidiary companies, can be handled more readily. On the other hand, you must ensure that the forest root domain controllers are carefully secured and protected against disaster because their loss effectively destroys the entire forest structure.

Best Practices

Planning the AD DS domain structure is an act that has far-reaching implications. This process is something that cannot simply be decided by a few network administrators sitting down with a few diagrams of the network and company business structures. Rather, it must involve the company's senior and middle management as well as business strategy specialists and representatives from remote offices. If you use internally developed applications, representatives of the development team should be involved. The following guidelines will help you make your AD DS implementation proceed smoothly:

Key Topic

- **Know everything there is to know about the network:** Although this guideline might sound intuitive for senior administrators who have built the network from the ground up, those who have come on the scene more recently need to gather information about everything that must be accounted for in an AD DS plan.
- **Employ a test lab:** The lab should contain representative domain controllers, member servers, and client computers. Set up a mini version of your complete network and engage the assistance of a representative set of users to test all facets of the implementation thoroughly.
- **Prepare thorough documentation:** This point can never be understated. Use tools such as Microsoft Visio to prepare diagrams of different levels of company detail, from the major administrative units down to the smallest workgroups. Visio is a tool that is specifically designed for preparing administrative diagrams such as those required in this scenario. This exercise also helps in optimizing communication between technical individuals and top management.
- **Use an email distribution list to keep everyone informed:** When all concerned individuals have full access to the latest developments, unpleasant surprises are minimized.
- **Keep all employees informed:** Although the regular workers might not understand the details of what is happening, they should be informed of the summary points of any planned changes. They will then be much more able to cope with the changes. In addition, they could provide valuable feedback.
- **Ensure that all top managers know what's happening:** This point also can never be understated. This helps prevent unpleasant surprises and the need to redo portions of the planning process.

- **Understand thoroughly the network's TCP/IP infrastructure:** Your understanding helps in designing the network and DNS configuration that is the foundation of the AD DS infrastructure. It is especially true in developing the proper site structure, as will be discussed in Chapter 6, "Configuring Active Directory Sites and Replication."
- **Develop and adhere to an adequate security policy:** Thoroughly review any security policy that your company already has in place. Apply the policy's constraints to the proper design of your company's domain structure. Make any appropriate changes as you develop the AD DS infrastructure.
- **Know the capabilities of your WAN links:** If your network includes slow WAN links, test and monitor the use of these links before and during the AD DS implementation to ensure that you have the optimum configuration.

Creating Forests and Domains

After you have created a comprehensive plan for your organization's AD DS structure, you are almost ready to begin the installation. The first task that you must perform is to install the first domain controller for the forest root domain.

Requirements for Installing Active Directory Domain Services

Before you can install AD DS, you must have at least one server that meets the following requirements:

Key Topic

- **Operating system:** The server must be running the Foundation, Standard, Enterprise, or Datacenter edition of Windows Server 2008 R2. Note that a server running the Web edition cannot act as a domain controller.
- **Adequate hard disk space:** Beyond the space used for installing Windows Server 2008 R2, the server must have a minimum of 500 MB of disk space for the Active Directory database and `SYSVOL` folder, plus at least 100 MB for the transaction log files. The larger the proposed network, the more disk space is necessary. And in practical terms, you should have several gigabytes of available space at a minimum. In Windows Server 2008 R2, you should have additional disk space for the following reasons:
  —The online defragmentation process is changed in Windows Server 2008 R2.
  —Windows Server 2008 R2 domain controllers have additional indices on the large link table.
  —The Active Directory Recycle Bin in Windows Server 2008 R2 holds deleted objects and their attributes until cleared.
- **A disk volume formatted with the NTFS file system:** This ensures security of the database; furthermore, it is required for the `SYSVOL` folder. Windows Server 2008 R2 creates an NTFS partition by default when installed.

TIP It is strongly recommend that you use a fault-tolerant disk volume such as RAID-1 (disk mirroring) or RAID-5 (disk striping with parity) for the Active Directory files. This enables the domain controller to function in the event of a disk failure, until the failed disk can be replaced. However, fault-tolerant disks are no substitute for regular backups of Active Directory. Backups are discussed in Chapter 15, "Maintaining Active Directory."

- **A DNS server:** Active Directory requires that a DNS server that supports service (SRV) resource records be present. This can be any server running Windows 2000 or later or a UNIX server running Berkeley Internet Name Domain (BIND) 4.9.7 or later. If you want to integrate the DNS database with Active Directory, you should install DNS on the same server that you install AD DS. If the Active Directory Installation Wizard cannot find a suitable DNS server, you will be prompted to install one. DNS is discussed in Chapter 2, "Installing and Configuring DNS for Active Directory," and Chapter 4, "Configuring DNS Server Settings and Replication."
- **Administrative privileges:** You must be logged on with an account that has the appropriate administrative privileges. For the first domain controller, this is a local administrator. To add a domain to an existing forest, you must be a member of the Enterprise Admins group in this forest; to add a domain controller to an exiting domain, you must be a member of the Domain Admins or Enterprise Admins group in this domain. Group memberships are discussed in Chapter 9, "Active Directory User and Group Accounts."

Installing Active Directory Domain Services

As in Windows 2000 and Windows Server 2003, Active Directory provides the Active Directory Installation Wizard (`dcpromo.exe`) that handles all aspects of installing or removing Active Directory. Windows Server 2008 is different from previous Windows Servers in that you install AD DS first and then install a domain controller. You can install AD DS without installing a domain controller if you are configuring your server for a directory-related application such as Exchange Server. This section looks at the use of this wizard for installing different types of domain controllers.

You can start the Active Directory Installation Wizard from the Add Roles Wizard in Server Manager or directly from the `dcpromo.exe` command. The following sections describe the use of the Add Roles Wizard for installing AD DS.

NOTE If you run `dcpromo.exe` without having first installed AD DS, Windows installs this service before starting the Active Directory Installation Wizard.

New Forests

As already noted, the first domain installed is the root domain in its forest. You must be a local administrator on the server on which you install Active Directory to proceed. The following procedure describes the installation of the first domain:

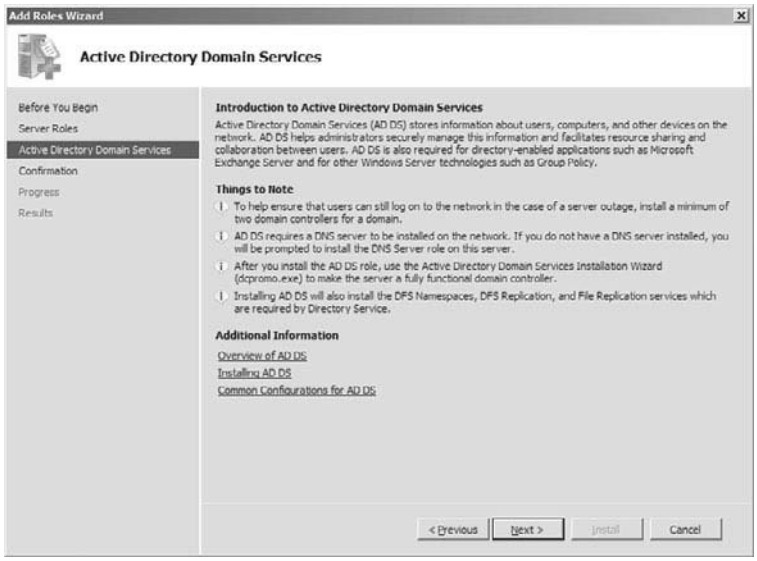
Step 1. In the Add Roles Wizard, select **Active Directory Domain Services** and then click **Next**.

Step 2. If you receive a message box labeled Add features required for Active Directory Domain Services and asking you to install .NET Framework 3.5.1, click **Add Required Features**.

Step 3. The wizard displays the Introduction to Active Directory Domain Services page shown in Figure 3-2. Make note of the points displayed by this page. If you want additional details regarding installation of Active Directory, click any of the links provided. When finished, click **Next**.

Figure 3-2 You can use the Add Roles Wizard to begin the installation of AD DS.

Key Topic



Step 4. Note the information provided on the Confirm Installation Selections page and then click **Install** to begin installing Active Directory.

Step 5. The wizard displays an Installation Progress page that charts the progress of installation. After a few minutes, it informs you that the AD DS role has been installed successfully and that you need to launch the Active Directory Domain Services Installation Wizard (`dcpromo.exe`). Click **Close** to exit the wizard and return to Server Manager.

Step 6. Scroll down to the Roles Summary section of Server Manager. Note that Active Directory Domain Services is shown as having been installed. A message marked with a red X indicates the number of system services that are not running.

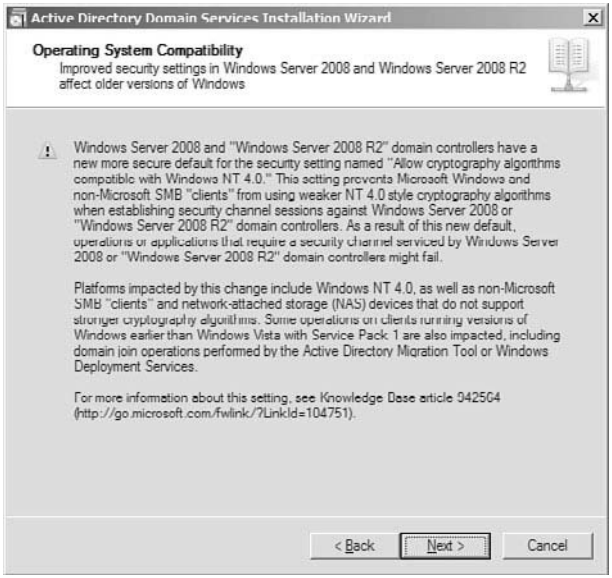
Step 7. Click this message. You are informed that the server is not yet running as a domain controller. Click the link provided to start the AD DS Installation Wizard.

Step 8. This wizard opens with a Welcome page. Click **Next**.

Step 9. The Operating System Compatibility page shown in Figure 3-3 informs you that Windows Server 2008 R2 security settings affect how older versions of Windows communicate with the domain controller. Access the Knowledge Base article quoted for more information. Click **Next** to proceed with AD DS installation.

Figure 3-3 You are informed about security settings that prevent some older Windows clients or non-Windows systems from logging on to the Windows Server 2008 R2 domain controller.

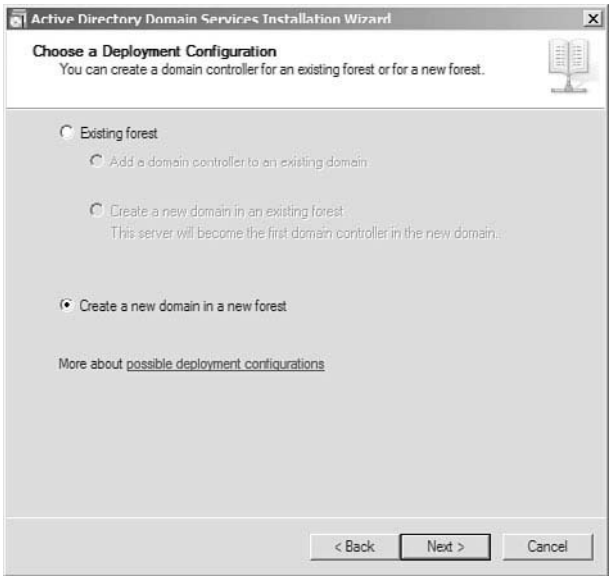
Key Topic



Step 10. On the Choose a Deployment Configuration page shown in Figure 3-4, select **Create a new domain in a new forest** and then click **Next**. On this page, you would select the **Existing forest** option when creating a new domain in an existing forest or adding a domain controller to an existing domain. These options are discussed later in this chapter.

Step 11. Type the full DNS name of the forest root domain and then click **Next**.

Figure 3-4 The wizard provides options for installing a domain controller in an existing forest or a new one.



NOTE Windows Server 2008 R2 no longer supports the creation of single-label domain names; however, you can still upgrade existing single-label domains to Windows Server 2008 R2. For more information, refer to "Information about configuring Active Directory domains by using single-label DNS names" at http://support.microsoft.com/kb/300684.

Step 12. The wizard verifies the forest and NetBIOS names and then displays the Set Forest Functional Level page shown in Figure 3-5. Select the appropriate forest functional level and then click **Next**. The available domain and forest functional levels are discussed later in this chapter.

Step 13. Select a domain functional level and then click **Next**.

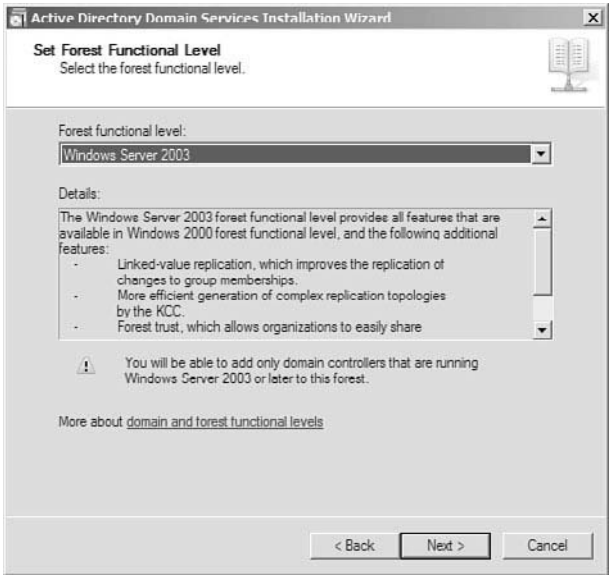
Step 14. The Additional Domain Controller Options page provides the following additional options that you can install for the domain controller. Ensure that **DNS Server** is selected and then click **Next**.

—**DNS Server:** Installs DNS on this server. This option is selected by default when first installing AD DS because DNS is required for Active Directory.

—**Global Catalog:** Installs a Global Catalog server. This option is not available but selected when installing the first domain controller in any domain because this server must be a global catalog server.

Figure 3-5 The wizard enables you to select from four forest functional levels.

Key Topic



—**Read-Only Domain Controller (RODC):** Installs an RODC. This option is not available because the first domain controller cannot be an RODC. Installing an RODC is discussed in Chapter 8, "Read-Only Domain Controllers."

Step 15. If the server does not have a statically assigned IP address, you are informed of this fact. A domain controller (and in particular, one that is configured as a DNS server) should always have a statically assigned IP address to ensure that client computers can always reach it. Select **Yes, open the IP properties so that I can assign a static IP address to the network adapter**, and then configure an appropriate IP address, subnet mask, default gateway, and default DNS server address.

Step 16. If you receive a message informing you that a delegation for the DNS server will not be created, click **Yes** to continue. You might receive this message if you are installing DNS on this server. If so, you should manually create this delegation later.

Step 17. Confirm the locations provided for the database, log files, and `SYSVOL` folders. If you want to change any of these locations, type the desired path or click **Browse**. When finished, click **Next**.

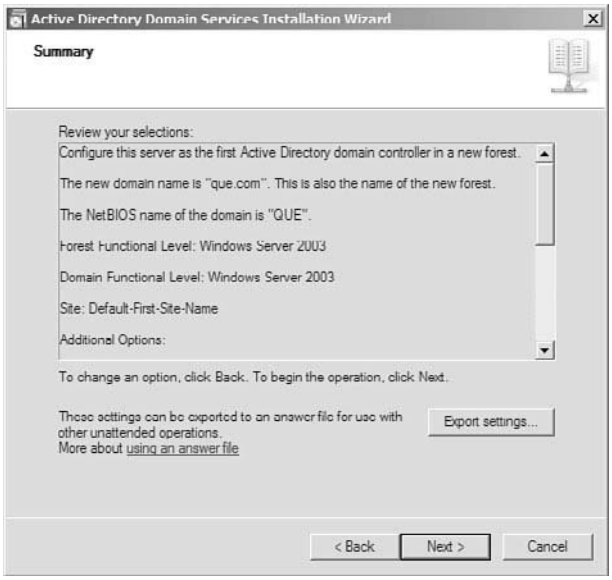
TIP When setting up a domain controller on a production network, it is advisable to place the database and log folders on a separate drive from the `SYSVOL` folder.

The reason for doing so is to improve only I/O performance; this does not improve security or fault tolerance, as an exam question might lead you to believe.

Step 18. On the Directory Services Restore Mode Administrator Password page, type and confirm a secure password. Make a careful note of the password you typed in case you need to use it later and then click **Next**.

Step 19. The wizard provides a Summary page as shown in Figure 3-6. Review the information provided on the Summary page. If you want to change any settings, click **Back** and make the appropriate changes. If you want to export information to an answer file, click **Export settings** and provide an appropriate path and filename. Then click **Next** to configure AD DS. This process takes several minutes.

Figure 3-6 The wizard provides a summary page that enables you to review the settings you've specified.



Step 20. When the completion page appears, click **Finish** and then click **Restart Now** to reboot your server. To reboot the server automatically, select the **Reboot on Completion** check box.

NOTE The Welcome page of the Active Directory Installation Wizard also contains an Advanced mode option. Select the check box provided to perform any of the following actions:

- Installing a domain controller from backup media created on an existing domain controller
- Modifying the NetBIOS name generated by default
- Selecting a source domain controller when installing an additional domain controller in the domain
- Defining a password replication policy that specifies the passwords cached on a read-only domain controller (RODC)

You can also invoke the Advanced mode directly from the `dcpromo` command by including the `/adv` parameter with this command.

New Domains in Existing Forests

After you have installed the forest root domain, you can add additional child domains or domain trees to the forest. Either procedure is similar to the procedure already outlined for creating a forest root domain, as follows:

Step 1. Follow the procedure to install AD DS and start the Active Directory Installation Wizard as described in the previous section until you receive the Choose a Deployment Configuration page previously shown in Figure 3-4.

Step 2. On this page, select **Existing forest**, and then select **Create a new domain in an existing forest**. Then click **Next**.

Step 3. On the Network Credentials page, type the name of the parent domain in which you want to install a child domain. Then click **Set** and specify the username and password of an account with the appropriate privileges described earlier in this chapter and click **Next**.

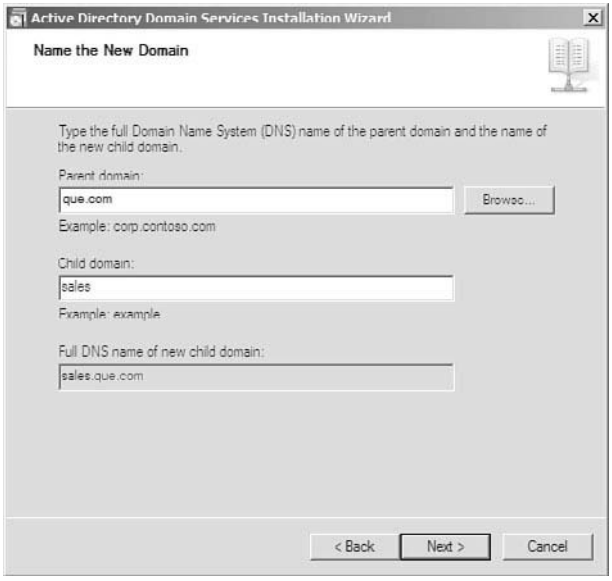
Step 4. On the Name the New Domain page shown in Figure 3-7, type the name of the parent and child domains in the spaces provided. The new domain will be created as a child domain or new tree automatically depending on the name you provide. Then click **Next**.

Step 5. On the Set Domain Functional Level page, select the required functional level and then click **Next**. Domain functional levels are discussed later in this chapter.

Step 6. On the Select a Site page, select an appropriate site and then click **Next**. Sites are discussed in Chapter 6.

Step 7. Complete the installation of the domain controller according to steps 14–20 of the previous procedure.

Figure 3-7 You create a child domain name from the name of the parent domain and the new top-level name on the Name the New Domain page.



Existing Domains

Installing additional domain controllers in an existing domain is important for the following reasons:

Key Topic

- Doing so adds fault tolerance and load balancing to the domain. In other words, additional domain controllers help share the load and improve performance.
- Users logging on to the domain can connect to any available domain controller for authentication.
- Users at a remote location can connect to a domain controller at their site rather than making a slow connection across a WAN link.
- If a domain controller should become unavailable because of a network or hardware failure, users can still log on to the domain.

To install an additional domain controller in an existing domain, follow the same procedure as in the previous section, except select the **Add a domain controller to an existing domain** option shown in Figure 3-4. Then select the proper domain from the Select a Domain page (this page will display all available domains in the forest). The remainder of the procedure is the same as that for creating a new domain in an existing forest, except that the Set Domain Functional Level page does not appear.

Performing Unattended Installations of Active Directory

Key Topic

Windows Server 2008 R2 enables you to specify parameters for Active Directory installation in an answer file that you can use to facilitate the installation of multiple domain controllers. This file is formatted as a simple text file containing the statement [DCINSTALL] on the first line followed by statements in the form *option=value*. Table 3-2 describes several of the more common options you can use in this file:

Table 3-2 Several Options Used for Unattended Domain Controller Installation

Option	Value	Meaning
`UserName`	Username of administrative user	Installs the domain controller in the context of this user.
`Password`	User's password | *	Specifies the password of the user installing the domain controller. Use * to prompt for the password.
`ReplicaOrNewDomain`	`Domain | Replica | ReadOnlyReplica`	Specifies whether to install a new domain, an additional domain controller (replica) in an existing domain, or an RODC in an existing domain.
`ReplicaDomainDNSName`	Existing domain name	Specifies the fully qualified domain name (FQDN) of the domain in which you are installing an additional domain controller.
`NewDomain`	`Forest | Tree | Child`	Specifies whether to install a new forest, a new tree in an existing forest, or a child domain.
`NewDomainDNSName`	Domain name to be created	Specifies the FQDN for a new domain.
`ParentDomainDNSName`	Parent domain name	Specifies the FQDN of the parent domain when creating a child domain.
`ChildName`	Child domain name	Specifies the top-level DNS name of the child domain. This name is prefixed to the parent name to create the FQDN of the child domain.

Table 3-2 Several Options Used for Unattended Domain Controller Installation

Option	Value	Meaning
ForestLevel	`0 | 2 | 3 | 4`	Specifies the forest functional level of a new forest: 0 = Windows 2000 2 = Windows Server 2003 3 = Windows Server 2008 4 = Windows Server 2008 R2
DomainLevel	`0 | 2 | 3 | 4`	Specifies the domain functional level of a new domain. Parameters have the same meaning as just described.
InstallDNS	`Yes | No`	Specifies whether a DNS server is installed.
ConfirmGC	`Yes | No`	Specifies whether the domain controller is installed as a global catalog server.
DatabasePath	Path to database folder	Default is `%systemroot%\NTDS.`
LogPath	Path to log folder	Default is `%systemroot%\NTDS.`
SysvolPath	Path to SYSVOL folder	Default is `%systemroot%\SYSVOL.`
RebootOnCompletion	Yes | No	Specifies whether to restart the computer on completion, regardless of success.

Many additional options are available, including options specific to the demotion of domain controllers. For additional information, consult "Appendix of Unattended Installation Parameters" at http://technet.microsoft.com/en-us/library/cc732086(WS.10).aspx.

To perform an unattended installation of a domain controller, open a command prompt and type the following command:

```
dcpromo /answer:path_to_answer_file
```

where *path_to_answer_file* specifies the complete path to the unattended answer file containing the parameters specified in Table 3-2. You can also include any of these parameters in the command line by prefixing each of them with the "/" character. The output to the command prompt will track the progress of the

promotion, and then the server will automatically reboot if the `RebootOnCompletion` parameter has been specified.

Server Core Domain Controllers

You cannot use Server Manager or a simple execution of `dcpromo` to promote a Server Core machine to a domain controller. You must use an unattended installation answer file in a similar manner to that described in the previous section. This file must include the information required to identify the domain being joined, including the username and password for a domain administrator account.

NOTE For further information on the use of Server Core, including its use as a domain controller, refer to "Server Core Installation Option of Windows Server 2008 Step-by-Step Guide" at http://technet.microsoft.com/en-us/library/cc753802(WS.10).aspx.

Removing Active Directory

The Active Directory Installation Wizard also enables you to remove Active Directory from a domain controller, thereby demoting it to a member server. Proceed as follows:

Step 1. Click **Start > Run**, type **`dcpromo`,** and then press **Enter.**

Step 2. Windows checks whether Active Directory Domain Services is installed and then displays the Welcome page. Click **Next**.

Step 3. If you receive a message warning you of the effects of removing a global catalog server, click **OK**.

Step 4. You receive the Delete the Domain page shown in Figure 3-8. Note all the warnings displayed about the effects of removing a domain. Select the check box only if you are removing the last domain controller from its domain and then click **Next**.

Step 5. You receive the Application Directory Partitions page if the server holds the last replica of any application directory partitions. Click **Next**, select the check box labeled **Delete all application directory partitions on this Active Directory domain controller**, and then click **Next** again to remove the application directory partitions.

Step 6. Type and confirm a password for the local Administrator account on the server, and then click **Next**.

Step 7. Read the information provided on the Summary page. If you need to make any changes, click **Back**. When ready, click **Next** to demote the server.

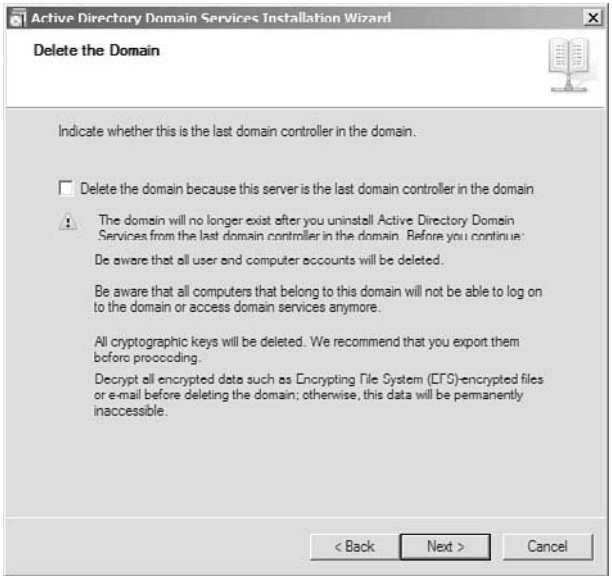


Figure 3-8 When you demote a domain controller, you are warned of the effects of deleting the domain.

Step 8. When the demotion is finished, click **Finish** and then click **Restart now** to restart the server. To reboot the server automatically, select the **Reboot on Completion** check box.

NOTE Although this procedure demotes the computer to a member server, it does not remove AD DS. If you want to remove AD DS after demoting the server, use the Remove Roles Wizard available from Server Manager after restarting the server.

Interoperability with Previous Versions of Active Directory

Many organizations have created Active Directory domains based on Windows 2000 or Windows Server 2003 domain controllers and are now in a position to take advantage of the new features of Windows Server 2008 and Windows Server 2008 R2 Active Directory. You can add new Windows Server 2008 domain controllers to an existing older Active Directory forest or upgrade all domain controllers in the forest to Windows Server 2008.

As summarized in Chapter 1, Active Directory in Windows Server 2008 and Windows Server 2008 R2 introduces numerous additional features not supported by previous versions of Windows Server. Many of these features limit the interoperability of Windows Server 2008 with previous versions, and Microsoft has

extended the concept of domain and forest functional levels to define the actions that can be done on a network that includes older domain controllers.

This section looks at these functional levels and the tools used for upgrading an older Active Directory network to Windows Server 2008.

Forest and Domain Functional Levels

As you noticed when installing your first domain controller (refer to Figure 3-5), Table 3-3 summarizes the forest and domain functional levels supported by Active Directory in Windows Server 2008.

Key Topic

Table 3-3 Forest and Domain Functional Levels in Windows Server 2008 R2 Active Directory

Forest Functional Level	Domain Functional Levels Supported	Domain Controllers Supported
Windows 2000 native	Windows 2000 native	Windows 2000
	Windows Server 2003 native	Windows Server 2003
	Windows Server 2008 native	Windows Server 2008
	Windows Server 2008 R2 native	Windows Server 2008 R2
Windows Server 2003 native	Windows Server 2003 native	Windows Server 2003
	Windows Server 2008 native	Windows Server 2008
	Windows Server 2008 R2 native	Windows Server 2008 R2
Windows Server 2008 native	Windows Server 2008 native	Windows Server 2008
	Windows Server 2008 R2 native	Windows Server 2008 R2
Windows Server 2008 R2 native	Windows Server 2008 R2 native	Windows Server 2008 R2

To make use of the functionality provided by Windows Server 2008 Active Directory, you must upgrade all domain controllers to Windows Server 2008 and upgrade the functional levels accordingly. A domain running at the Windows Server 2008 domain functional level located in a forest running at a lower functional level supports domain-based Windows Server 2008 Active Directory features but not forest-based ones.

Furthermore, to make use of the newest Active Directory features in Windows Server 2008 R2, you must upgrade all domain controllers to Windows Server 2008 R2 and upgrade the domain and forest functional levels accordingly.

NOTE You can deploy an RODC to a domain in which the domain and forest functional levels are set to Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.

Windows Server 2008 does not support the Windows 2000 mixed functional level previously found in older Active Directory networks. If you still have any domain controllers running Windows NT 4.0, you must upgrade or remove these domain controllers before introducing a Windows Server 2008 or Windows Server 2008 R2 domain controller on your network.

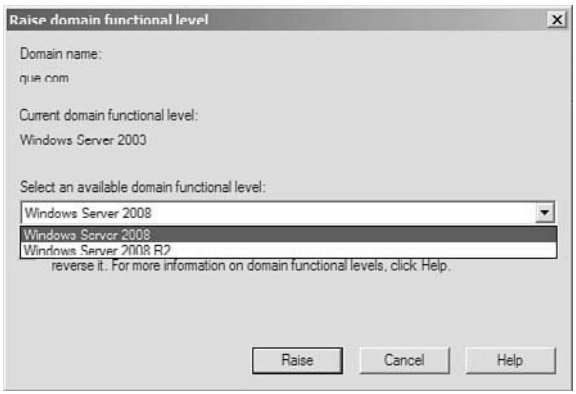
Upgrading Domain and Forest Functional Levels

To raise the forest functional level, you must first raise the functional level of all domains in the forest to the same or higher domain functional level. To raise the domain functional level, perform any of the following three actions:

- Open the Active Directory Administrative Center snap-in, right-click your domain, and then choose **Raise the domain functional level**.
- Open the Active Directory Users and Computers snap-in. Right-click **Active Directory Users and Computers** and choose **All Tasks > Raise domain functional level**.
- Open the Active Directory Domains and Trusts snap-in, right-click your domain, and choose **Raise domain functional level**.

In the dialog box shown in Figure 3-9, select the appropriate functional level and click **Raise**. Then click **OK** to accept the warning that is displayed.

Figure 3-9 Raising the domain functional level.



To raise the forest functional level, access the Active Directory Domains and Trusts snap-in. Right-click **Active Directory Domains and Trusts** and select **Raise forest functional level**. Select the appropriate functional level, click **Raise**, and then click **OK** to accept the warning that is displayed. You can also right-click your domain name in the Active Directory Administrative Center and choose **Raise the forest functional level** and then follow the same procedure described here.

WARNING It is important to remember that raising forest and domain functional levels is a one-way operation. You cannot go back to a lower functional level. In addition, you cannot introduce an older domain controller after you have raised the domain functional level.

NOTE For additional information on domain and forest functional level upgrades, refer to "Identifying Your Functional Level Upgrade" at http://technet.microsoft.com/en-us/library/cc754209(WS.10).aspx.

Key Topic

The **Adprep** Utility

Microsoft provides the `Adprep` utility to prepare a down-level Active Directory domain for receiving Windows Server 2008 and Windows Server 2008 R2 domain controllers. Found in the `\sources\adprep` folder of the installation DVD-ROM, this tool prepares the forest and domain by extending the Active Directory schema and updating several required permissions.

Running the **Adprep /forestprep** Command

You must run the `Adprep /forestprep` command on the schema master of the forest first. It extends the schema to receive the new Windows Server 2008 enhancements, including the addition of directory descriptors for certain objects including granular password policies. You have to run this command and let its changes replicate throughout the forest before you run the `Adprep /domainprep` command. To run this command, you must be a member of the Enterprise Admins, Schema Admins, and Domain Admins groups in the forest root domain.

WARNING Before running this command, ensure that any Windows 2000 domain controllers are upgraded to SP2 or later, or at least to SP1 with hotfix QFE265089. Refer to Microsoft Knowledge Base article 331161 for more information.

Running the **`Adprep /domainprep`** Command

Run the `Adprep /domainprep` command on the infrastructure master of each domain in which you plan to introduce Windows Server 2008 domain controllers. It adjusts access control lists (ACLs) on Active Directory objects and on the `SYSVOL` shared folder for proper access by Windows Server 2008 domain controllers. To run this command, you must be a member of the Domain Admins group in the respective domain and the domain must be operating at the Windows 2000 Server native mode or higher.

You can also run the `Adprep /domainprep /prep` command to include updates required for enabling Resultant Set of Policy (RSoP) planning mode functionality.

TIP Remember that you must run `adprep /forestprep` on the schema master and that you must run this command before you run `adprep /domainprep`. Also remember that you must run `adprep /domainprep` on the infrastructure master of each domain in which you want to introduce a Windows Server 2008 domain controller and that you must complete these commands before promoting or upgrading an existing domain controller.

Upgrading a Windows Server 2003 Domain Controller

You can also upgrade an existing Windows Server 2003 domain controller to Windows Server 2008. See Appendix B, "Installing Windows Server 2008 R2," for information on upgrading Windows Server 2003 computers; the procedure outlined in this chapter automatically upgrades AD DS to Windows Server 2008. However, you cannot upgrade a Windows 2000 domain controller to Windows Server 2008 directly; you must first upgrade to Windows Server 2003 and then to Windows Server 2008.

Note that to upgrade a Windows Server 2003 domain controller to Windows Server 2008, you must first run the `Adprep` utility as already discussed to upgrade the schema for accepting Windows Server 2008 domain controllers.

You can upgrade a Windows Server 2003 domain controller to Windows Server 2008 R2, provided the server meets the hardware requirements discussed in Appendix B.

Before upgrading the first Windows Server 2003 domain controller, ensure that you have run the `Adprep /forestprep` and `Adprep /domainprep` commands and that these commands have completed without error. Then select the **Install now** command from the Welcome screen displayed by the Windows Server 2008 R2 DVD-ROM, and follow the instructions provided by the Installation Wizard and summarized in Appendix B, "Memory Tables".

Additional Forest and Domain Configuration Tasks

This section introduces two additional configuration tasks specified in the Exam 70-640 objectives for configuring a forest or domain: use of the Active Directory Migration Tool (ADMT) v.3.1 and the alternative user principal name (UPN) suffix. Before introducing these tasks, we take a quick look at some procedures that verify that AD DS has been properly installed and, in doing so, introduce some to the administrative tools included with AD DS.

Verifying the Proper Installation of Active Directory

After you have installed Active Directory, there are several steps you should perform to verify that the proper components have been installed. Click **Start > Administrative Tools**. On a Windows Server 2008 R2 computer, you should see links to five Active Directory management tools: Active Directory Administrative Center, Active Directory Domains and Trusts, Active Directory Module for Windows PowerShell, Active Directory Sites and Services, and Active Directory Users and Computers. You should also see a link to the DNS snap-in unless you have specified another server as the DNS server for your domain.

Open Active Directory Users and Computers. You should see the default containers Builtin, Computers, ForeignSecurityPrincipals, Managed Service Accounts, and Users under the domain you have created. You should also see a default Domain Controllers OU. Select this OU and verify that computer accounts for all domain controllers in the domain are present, as shown in Figure 3-10.

On a Windows Server 2008 R2 computer, open Active Directory Administrative Center. As shown in Figure 3-11, this new MMC snap-in enables you to perform a large range of administrative tasks on your domain, including the following:

- Creating and managing user, group, and computer accounts
- Creating and managing OUs and other Active Directory containers
- Managing other trusted AD DS domains
- Using query-building searches to filter AD DS data

Uses of this tool will be discussed throughout this *Cert Guide* as appropriate, together with references to tools used on Windows Server 2008 computers that are not running R2.

Figure 3-10 After installing Active Directory, you should see a default set of containers in the Active Directory Users and Computers, together with domain controller computer accounts in the Domain Controllers OU.

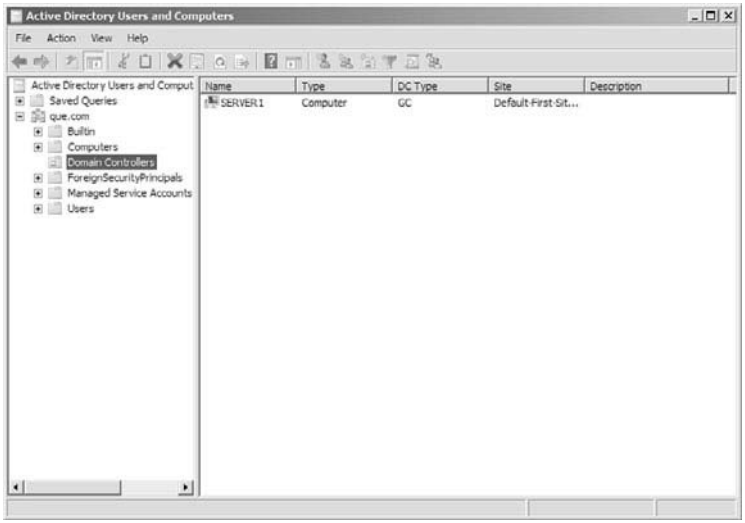
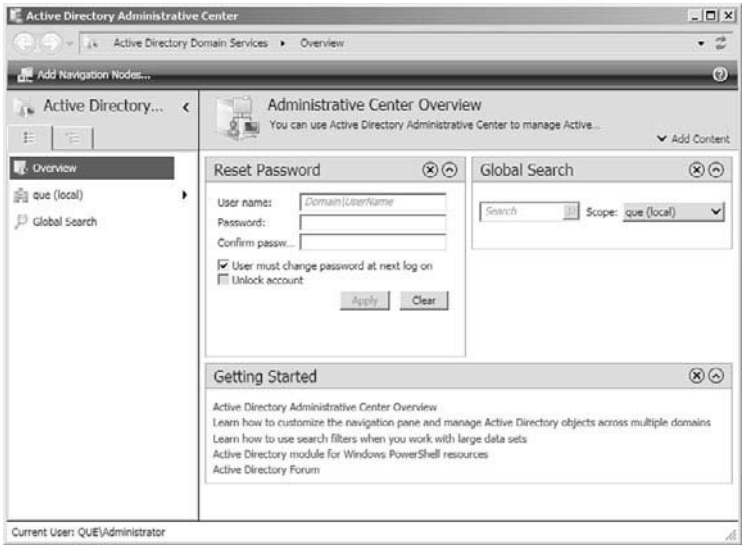


Figure 3-11 Windows Server 2008 R2 adds the Active Directory Administrative Center to the suite of tools provided for administering AD DS.



NOTE In this discussion and elsewhere in this book, the term *Windows Server 2008* is taken to include both the original and R2 versions unless otherwise noted. The term *Windows Server 2008 R2* is used when referring to new features added with this version of the server software.

The Active Directory Administrative Center is installed automatically when you install the AD DS server role in Windows Server 2008 R2. You can also install this tool on a Windows Server 2008 R2 member server or a Windows 7 computer by installing the Remote Server Administration Tools (RSAT) feature. You cannot, however, install Active Directory Administrative Center on a computer running the original version of Windows Server 2008 or on older versions of Windows Server.

NOTE For an overview of the capabilities of the Active Directory Administrative Center, refer to "What's New in AD DS: Active Directory Administrative Center" at http://technet.microsoft.com/en-us/library/dd378856(WS.10).aspx.

Active Directory Migration Tool v.3.1

ADMT v.3.1 is the most recent version of a utility, available for download from the Microsoft website, which assists you in migrating objects such as users, groups, and computers between Active Directory domains in the same forest or in different forests. This tool assists you in the potentially difficult task of restructuring your AD DS forest structure; for example, when changes in your organization's business structure occur because of mergers, acquisitions, or divestitures. You can migrate these objects from a source domain running at any functional level of Windows 2000 native or higher to a target domain running at any functional level of Windows 2000 native or higher. If the source and target domains are in different forests, you must configure trust relationships between the domains in use to ensure data security during the migration process.

Actions performed by ADMT include the following:

- Ensures security of objects being migrated by using 128-bit encryption with the Passport Export Server (PES) service
- Preserves the SID history of objects being migrated
- Enables migration of user profiles
- Migrates computer accounts including domain controllers
- Enables the restructuring of Active Directory domains between forests
- Enables you to use a preconfigured SQL database to hold migration information
- Enables you to perform test migrations so that you can ensure the actual migration will run properly
- Provides a log file that you can check for migration errors and other problems
- Provides for rollback options in the event that the migration does not proceed properly
- Facilitates the decommissioning of old domains in forests to be removed

NOTE If you are migrating from or restructuring Windows NT 4.0 domains to Active Directory, you should use the 3.0 version of ADMT. You can use version 3.0 when restructuring a series of Windows NT 4.0 domains (such as account and resource domains structured into a multiple trust model) into a single Active Directory domain. Version 3.0 runs on Windows 2000 and Windows Server 2003 computers only; it does not run on Windows Server 2008 computers.

ADMT 3.1 runs on a server running the original edition of Windows Server 2008 only; it does not run on Windows Server 2008 R2. To use ADMT 3.1, navigate to http://www.microsoft.com/downloads/details.aspx?familyid=AE279D01-7DCA-413C-A9D2-B42DFB746059&displaylang=en and click the **Download** button. Then follow the instructions provided to download and save the `admtsetup31.exe` file to an appropriate location on your computer. Double-click the file, click **Run**, and then follow the instructions provided to install ADMT 3.1.

NOTE For more information on ADMT 3.1, refer to "ADMT v3.1 Guide: Migrating and Restructuring Active Directory Domains" at http://www.microsoft.com/downloads/en/confirmation.aspx?familyId=6d710919-1ba5-41ca-b2f3-c11bcb4857af&displayLang=en. For information on use of ADMT 3.1 in domains with Windows Server 2008 R2 domain controllers, refer to "Known issues that may occur when you use ADMT 3.1 to migrate to a domain that contains Windows Server 2008 R2 domain controllers" at http://support.microsoft.com/kb/976659.

Alternative User Principal Name Suffixes

As mentioned earlier in this chapter, a UPN is a logon name specified in the format of an email address such as user@examcram.com. It is a convenient means of logging on to a domain from a computer located in another domain in the forest or a trusted forest. Two types of UPNs are available:

- **Implicit UPN:** This UPN is always in the form *`user@domain`*, such as `peter@sales.que.com`. It is defined on the Account tab of a user's Properties dialog box in Active Directory Users and Computers.
- **Explicit UPN:** This UPN is in the form *`string1@string2`*, where an administrator can define values for each string. For example, a user named Peter in the `sales.que.com` domain could have an explicit UPN in the form `peter@sales`. Using explicit UPNs is practical when an organization does not want to reveal its internal domain structure.

Windows Server 2008 supports the principle of the UPN suffix, first introduced in Windows Server 2003. This is the portion of the UPN to the right of the at (@) character. By default, the UPN suffix is the DNS domain name of the domain in which the user account is located.

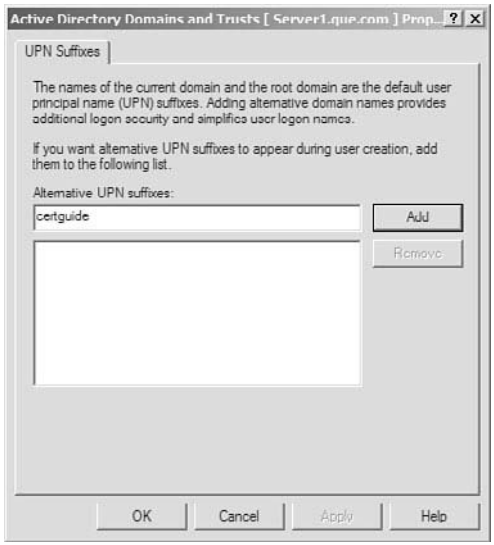
Adding an alternative UPN suffix provides several advantages:

- You can use a common UPN suffix across all users in a forest. This is especially useful if some users have long domain names.
- The UPN suffix enables you to conceal the actual domain structure of the forest from external users.
- You can use separate UPN suffixes in situations where different divisions of a company have separate email domain names, thereby enabling users to log on with a name that matches their email address.

To define an alternative UPN suffix, access Active Directory Domains and Trusts from the Administrative Tools folder. Right-click **Active Directory Domains and Trusts** and click **Properties**. From the Properties dialog box shown in Figure 3-12, type the name of the alternative UPN suffix desired, click **Add**, and then click **OK**. After you have done this, the alternative UPN suffix is available when you are configuring new or existing user accounts. For more information on configuring user accounts, see Chapter 9.

Figure 3-12 You can configure alternative UPN suffixes from the Active Directory Domains and Trusts Properties dialog box.

Key Topic



Exam Preparation Tasks

Review All the Key Topics

Key Topic

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 3-4 lists a reference of these key topics and the page numbers on which each is found.

Table 3-4 Key Topics for Chapter 3

Key Topic Element	Description	Page Number
List	Lists important guidelines you should follow in preparing to install AD DS	80
List	Summarizes requirements for installing AD DS	81
Figure 3-2	You use the Add Roles Wizard to begin the installation of AD DS	83
Figure 3-3	Displays important security considerations when installing AD DS	84
Figure 3-5	Selecting a forest functional level	86
List	Summarizes important reasons for installing multiple domain controllers in a domain	89
Paragraph	Describes the methods of performing unattended installations of AD DS	90
Table 3-3	Summarizes available forest and domain functional levels in Windows Server 2008 R2	94
Paragraph	Describes the `adprep` utility used for preparing forests and domains for upgrade	96
Figure 3-12	Specifying additional UPN suffixes	102

Complete the Tables and Lists from Memory

Print a copy of Appendix C, "Memory Tables" (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, "Memory Tables Answer Key," also on the CD, includes completed tables and lists to check your work.

Definitions of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary.

Active Directory Migration Tool (ADMT), Active Directory Administrative Center, `Adprep`, `dcpromo`, domain controller (DC), domain functional level, forest functional level, forest root, read-only domain controller (RODC), Server Core, universal principal name (UPN), universal principal name (UPN) suffix

This page intentionally left blank

Index

B

C

D

E

F

G

H

I-J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Z

This page intentionally left blank

This page intentionally left blank