



The Real

MCITP Windows Server 2008 Enterprise Administrator

Exam 70-647

PREP KIT

- **The Independent Source:** This is the independent source of exam-day tips, techniques, and warnings.
- **Guaranteed Coverage of All Exam Objectives:** This comprehensive study guide guarantees 100% coverage of all Microsoft's exam objectives.
- **Designed to Help You Prepare:** This package includes access to two Exam-Day Practice Exams, audio Fast Tracks for iPods or MP3 players, and a BONUS 1,000-page "DRILL DOWN" reference.

Tony Piltzecker Technical Editor

Tariq Azad

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of valueadded features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

This page intentionally left blank

The Real MCITP Exam 647 Windows Server 2008 Enterprise Administrator Prep Kit

Tony Piltzecker Technical Editor

Tariq Azad

Elsevier, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media® and Syngress®, are registered trademarks of Elsevier, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

| KEY | SERIAL NUMBER |
|-----|---------------|
| 001 | HJIRTCV764 |
| 002 | PO9873D5FG |
| 003 | 829KM8NJH2 |
| 004 | BPOQ48722D |
| 005 | CVPLQ6WQ23 |
| 006 | VBP965T5T5 |
| 007 | HJJ863WD3E |
| 008 | 2987GVTWMK |
| 009 | 629MP5SDJT |
| 010 | IMWQ295T6T |

PUBLISHED BY

Syngress Publishing, Inc.

Elsevier, Inc.

30 Corporate Drive

Burlington, MA 01803

The Real MCITP Exam 70-647 Prep Kit

Copyright © 2008 by Elsevier, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-249-2

Publisher: Andrew Williams

Acquisitions Editor: David George

Technical Editor: Tony Piltzcker

Project Manager: Gary Byrne

Cover Designer: Michael Kavish

Page Layout and Art: SPI

Copy Editors: Alice Brzovic, Adrienne Rebello, and Mike McGee

Indexer: Michael Ferreira

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

Technical Editor

Tony Piltzecker (CISSP, MCSE, CCNA, CCVP, Check Point CCSA, Citrix CCA), author and technical editor of Syngress Publishing's *MCSE Exam 70-296 Study Guide and DVD Training System* and *How to Cheat at Managing Microsoft Operations Manager 2005*, is an independent consultant based in Boston, MA. Tony's specialties include network security design, Microsoft operating system and applications architecture, and Cisco IP Telephony implementations. Tony's background includes positions as Systems Practice Manager for Presidio Networked Solutions, IT Manager for SynQor Inc, Network Architect for Planning Systems, Inc., and Senior Networking Consultant with Integrated Information Systems. Along with his various certifications, Tony holds a bachelor's degree in business administration. Tony currently resides in Leominster, MA, with his wife, Melanie, and his daughters, Kaitlyn and Noelle.

Lead Author

Tariq Bin Azad is the Principal Consultant and Founder of NetSoft Communications Inc., a consulting company located in Toronto, Canada. He is considered a top IT professional by his peers, coworkers, colleagues, and customers. He obtained this status by continuously learning and improving his knowledge and information in the field of information technology. Currently, he holds more than 100 certifications, including MCSA, MCSE, MCTS, MCITP (Vista, Mobile 5.0, Microsoft Communications Server 2007, Windows 2008, and Microsoft Exchange Server 2007), MCT, CIW-CI, CCA, CCSP, CCEA, CCI, VCP, CCNA, CCDA, CCNP, CCDP, CSE, and many more. Most recently, Tariq has been concentrating on Microsoft Windows 2000/2003/2008, Exchange 2000/2003/2007, Active Directory, and Citrix implementations. He is a professional speaker and has trained architects, consultants, and engineers on topics such as Windows 2008 Active Directory, Citrix Presentation Server, and Microsoft Exchange 2007. In addition to owning and operating an independent consulting company, Tariq works as a Senior Consultant and has utilized his training skills in numerous workshops, corporate trainings, and presentations. Tariq holds a Bachelor of Science in Information Technology from Capella University, USA, a Bachelor's degree in Commerce from University of Karachi, Pakistan, and is working on his ALMIT (Master's of Liberal Arts in Information Technology) from Harvard University, in Cambridge, MA. Tariq has been a coauthor on multiple books, including the best-selling *MCITP: Microsoft Exchange Server 2007 Messaging Design and Deployment Study Guide: Exams 70-237 and 70-238* (ISBN: 047018146X) and *The Real MCTS/MCITP Exam 640 Preparation Kit* (ISBN: 978-1-59749-235-5). Tariq has worked on projects or trained for major companies and organizations, including Rogers Communications Inc., Flynn Canada, Cap Gemini, HP, Direct Energy, Toyota Motors, Compaq, IBM, Citrix Systems Inc., Unicom Technologies, Amica Insurance Company, and many others. He lives in Toronto, Canada, and would like to thank his father, Azad Bin Haider, and his mother, Sitara Begum, for his lifetime of guidance for their understanding and support to give him the skills that have allowed him to excel in work and life.



Contributing Authors

Steve Magowan is a Senior IT Consultant with extensive experience in IT environment migrations and version upgrades for the Exchange and Active Directory resources of enterprise-level clients. As a result of corporate acquisitions Steve has also accomplished multiple large-scale Exchange, Active Directory, and application-based resource integration projects of companies in the 5,000- to 10,000-user range into larger 25,000+ user enterprise environments. In support of these projects, Steve has gained considerable exposure to the virtualization solutions offered by VMware, Citrix, and Microsoft. Working most extensively with VMware-based technologies, Steve has utilized virtualization platforms to accomplish large-scale physical-to-virtual application base server migrations, involving hundreds of application workloads. The use of virtualization technology has allowed Steve to successfully complete these integration initiatives in an efficient manner that was always invisible to end users. A retired veteran of the Canadian Air Force, Steve has spent the last 12 years building his IT skill set as a consultant. Since leaving the Air Force Steve has had the opportunity to perform migration and integration projects both in and outside of North America. His fluency in French and Spanish has allowed him to branch out and work in other parts of the world, providing the secondary benefit of travel, as well as the opportunity to work with and learn about people of other cultures and their languages. For Steve these expatriate experiences have been very valuable, and he is grateful to have had them.

Ryan Hanisco (MCSE, MCTS: SQL) is an Engagement Manager for Magenic, a company focused on delivering business value through applied technology and one of the nation's premier Microsoft Gold Certified Partners. Ryan has worked in the IT industry for over 10 years providing infrastructure and development services to organizations in

both the public and private sectors. He is a regular contributor to the Microsoft communities and believes strongly in supporting the community through thought leadership and open sharing of ideas. He has spoken at several national conferences on topics in varying disciplines, including Microsoft Vista deployment, Citrix implementation, and TCO of Terminal Service solutions. Ryan also maintains a technical blog, which proves technical and business best practices to bridge the gap between corporate strategy and IT's ability to execute. Ryan would like to thank Drew, Cinders, and Gato for putting up with him. Additional thanks go to Norm, Paul, John, Tom, Keith, and all the other Magenicons who keep me laughing and make IT a great industry to be in.

Joe Lurie (MCSE, MCT, MCTS, MCITP) is a Senior Consultant specializing in Microsoft Application Virtualization, Business Desktop Deployment, and Active Directory and has spent the past several years training thousands of students on these technologies. Joe holds several certifications from Microsoft, Cisco, and CompTia, and has been coaching students on exam prep since he first got certified in Windows NT. In addition to teaching, Joe was only the second person in North America to be certified to teach Microsoft Application Virtualization, and he has been consulting on this product since it was acquired by Microsoft. He also writes Hands-On-Labs for Microsoft and is frequently a Technical Learning Guide and presenter at many technical conferences, including Tech Ed, Tech Ready, and Launch Events. Besides Hands-On-Labs, a number of the Server 2008 First-Look clinics were either written or reviewed by Joe, as were dozens of Hand-On-Labs in technologies ranging from application compatibility, Windows Vista deployment, QoS, and group policy enhancements in Windows Server 2008. In his spare time, Joe has a wife and two daughters that he loves to spend time with, doing everything from reading to swimming to skiing. Joe is thankful to HynesITe, Axis Technology, and to the MCT community for the countless opportunities they have given him.

Christian Schindler is a Microsoft Certified Architect | Messaging, MCSE, MCITP for Windows Server 2008 and a MCT. He has been a trainer for 10 years and designed several customized courses for leading learning providers. He began his career as a systems engineer at a telecommunications company, managing directory and messaging services. Currently, he works as a Senior Consultant at NTx BackOffice Consulting Group, a Microsoft Gold Certified Partner specializing in advanced infrastructure solutions.

Shoab Syed is an expert in Microsoft Technologies. He has an extensive background in providing systems solutions and implementations spanning over 12 years. His clients include major national and international companies from various industries in both public and private sectors. Shoab currently resides in Toronto, Canada, and provides consulting services worldwide.

This page intentionally left blank

Contents

| | |
|---|--------------|
| Foreword | xxvii |
| Chapter 1 Name Resolution and IP Addressing | 1 |
| Introduction | 2 |
| Windows 2008 Name Resolution Methods..... | 2 |
| Developing a Naming Strategy | 2 |
| Comparing Name Resolution Procedures..... | 3 |
| Internal Names..... | 4 |
| External Names | 4 |
| Domain Name System | 5 |
| Host Names..... | 5 |
| Domain Names | 5 |
| Fully Qualified Domain Name (FQDN) | 6 |
| Is DNS Required? | 8 |
| DNS Queries | 9 |
| The DNS Query Process | 10 |
| Part 1: The Local Resolver | 10 |
| Part 2: Querying a DNS Server | 11 |
| Query Response Types | 14 |
| DNS Resource Records | 15 |
| DNS Zones | 17 |
| Non Active Directory–Integrated Zones | 19 |
| Zones Integrated with Active Directory..... | 21 |
| Secondary Zones, Stub Zones, and Condition Forwarding | 23 |
| The GlobalNames Zone | 23 |
| DNS Design Architecture | 24 |
| Split-Brain Design: Same Internal and External Names | 24 |
| Separate Name Design: Different External and Internal Names | 26 |
| DNS Server Implementation | 27 |
| DNS Dynamic Updates and Security | 32 |
| Creating Zones and Host Records | 33 |
| Setting Aging and Scavenging | 35 |
| Configuring DNS Client Settings | 38 |
| Setting Computer Names | 39 |
| NetBIOS Names Accommodation | 40 |
| Setting the Primary DNS Suffix..... | 40 |

| | |
|---|-----------|
| Setting Connection-Specific DNS Suffixes | 40 |
| The DNS Resolver Cache | 43 |
| Nslookup | 44 |
| Integration with WINS | 44 |
| The HOSTS File | 46 |
| Configuring Information for WINS Clients | 48 |
| WINS Name Registration and Cache | 51 |
| Setting Up a WINS Server | 52 |
| Configuring WINS Server | 53 |
| Configuring Replication Partners | 56 |
| Specifying Designated Replication Partners | 58 |
| Maintaining WINS | 60 |
| Burst Handling | 60 |
| Scavenging Records | 63 |
| The LMHOSTS File | 63 |
| TCP/IP v4 and v6 Coexistence | 65 |
| Features and Differences from IPv4 | 66 |
| Summary of Exam Objectives | 68 |
| Exam Objectives Fast Track | 69 |
| Exam Objectives Frequently Asked Questions | 74 |
| Self Test | 76 |
| Self Test Quick Answer Key | 80 |
| Chapter 2 Designing a Network Access Strategy | 81 |
| Introduction | 82 |
| Network Access Policies | 82 |
| Network Access Methods | 83 |
| Local Network Access | 84 |
| Remote Network Access | 85 |
| RADIUS Server | 85 |
| RADIUS Components | 87 |
| Network Policy and Access Services | 89 |
| NAP Client Components | 92 |
| Network Policy Server | 94 |
| Designing a Network for NAP | 103 |
| RADIUS Proxy Server | 104 |
| Remote Access Strategies | 105 |
| Terminal Services for Server 2008 | 105 |
| New Roles | 113 |
| Developing a Terminal Services Remote Access Strategy | 115 |

| | |
|--|-----|
| The Corporate Desktop | 116 |
| RemoteApp Programs | 117 |
| Terminal Services Licensing | 122 |
| Installing a Terminal Service Licensing Server | 122 |
| Installing the TS Licensing Role Service on an Existing Terminal Server | 123 |
| Installing the TS Licensing Role Service on a Separate Server | 124 |
| Activating a Terminal Service Licensing Server | 125 |
| Activating a Terminal Service Licensing Server Using the Automatic Connection Method | 126 |
| Activating a Terminal Service Licensing Server Using the Web Browser Method | 129 |
| Activating a Terminal Service Licensing Server Using the Telephone Method | 130 |
| Establishing Connectivity between Terminal Server and Terminal Services Licensing Server | 131 |
| Using the Terminal Services Configuration Tool to Specify a TS Licensing Server | 133 |
| Publishing a Terminal Services Licensing Server | |
| Using TS Licensing Manager | 134 |
| TS CAL Types | 134 |
| Locating Terminal Services Licensing Services | 135 |
| Launching and Using the Remote Desktop Connection Utility | 138 |
| Configuring the Remote Desktop Connection Utility | 139 |
| The General Tab | 139 |
| The Display Tab | 140 |
| The Local Resources Tab | 140 |
| The Programs Tab | 143 |
| The Experience Tab | 143 |
| The Advanced Tab | 145 |
| Terminal Services Troubleshooting | 145 |
| Routing and Remote Access | 148 |
| Virtual Private Networking | 150 |
| VPN Authentication Protocols | 150 |
| PPTP | 152 |
| Prerequisites | 152 |
| Pros | 152 |
| Cons | 153 |
| L2TP/IPSec | 153 |

| | |
|---|------------|
| Prerequisites | 153 |
| Pros. | 153 |
| Cons. | 154 |
| SSTP. | 154 |
| Prerequisites | 154 |
| Pros. | 155 |
| Cons. | 155 |
| Monitoring and Maintaining NPAS | 159 |
| Working with Perimeter Networks | 160 |
| Understanding Perimeter Networks. | 162 |
| Developing a Perimeter Network Strategy. | 164 |
| Benefits of Server Core. | 164 |
| Using Windows Firewall with Advanced Security. | 166 |
| Connection Security Rules | 166 |
| Firewall Rules | 167 |
| Server and Domain Isolation | 169 |
| Benefits of Server Isolation | 170 |
| Benefits of Domain Isolation. | 171 |
| Developing an Isolation Strategy | 172 |
| Summary of Exam Objectives. | 174 |
| Exam Objectives Fast Track | 175 |
| Exam Objectives Frequently Asked Questions | 178 |
| Self Test. | 181 |
| Self Test Quick Answer Key | 184 |
| Chapter 3 Active Directory Forests and Domains | 185 |
| Introduction | 186 |
| New in Windows Server 2008 Active Directory | |
| Domain Services. | 186 |
| Designing Active Directory Forests and Domains. | 193 |
| Factors to Consider When Creating Forest Design Plans. | 193 |
| Business Units | 193 |
| Schema | 194 |
| Legal. | 194 |
| Security. | 194 |
| Namespaces. | 194 |
| Timelines | 195 |
| Administrative Overhead | 195 |
| Testing Environments. | 196 |
| Creating a Design Plan | 196 |

| | |
|---|-----|
| The Forest Structure | 199 |
| The Active Directory Domain Services (AD DS) | |
| Logical Design Structure | 199 |
| Active Directory Forest | 200 |
| Active Directory Tree | 201 |
| Active Directory Domain | 201 |
| Organizational Units (OU) | 202 |
| The Active Directory Domain Services (AD DS) Physical | |
| Design Structure | 204 |
| Domain Controllers | 204 |
| Sites and Site Links | 204 |
| Subnets | 205 |
| Creating the Forest Root Domain | 206 |
| Forest and Domain Function Levels | 209 |
| Upgrading Your Forest | 213 |
| Windows 2000 Native Mode Active Directory to | |
| Windows Server 2008 AD DS | 213 |
| Windows Server 2003 Forest to Windows Server 2008 | 214 |
| New Forest | 215 |
| Intra-Organizational Authorization and Authentication | 215 |
| Schema Modifications | 218 |
| Designing an Active Directory Topology | 220 |
| Server Placement | 222 |
| Determining the Placement of the Forest Root | |
| Domain Controllers | 222 |
| Determining the Placement of the Regional | |
| Domain Controllers | 222 |
| Determining the Placement of the Operations Masters | 224 |
| Placement of the PDC Emulator | 225 |
| Placement of the Infrastructure Master | 225 |
| Planning for Networks with Limited Connectivity | 226 |
| Determining the Placement of Global Catalog Servers | 228 |
| Creating the Site Link Objects | 231 |
| Site Link Bridge Design | 233 |
| Creating the Site Objects | 234 |
| Creating the Subnet Objects | 235 |
| Printer and Location Policies | 235 |
| Designing an Active Directory Administrative Model | 239 |
| Delegation | 240 |

| | |
|--|-----|
| Group Strategy | 241 |
| Compliance Auditing | 245 |
| Global Audit Policy | 247 |
| SACL | 247 |
| Schema | 248 |
| Summary of Exam Objectives | 249 |
| Exam Objectives Fast Track | 250 |
| Exam Objectives Frequently Asked Questions | 253 |
| Self Test | 254 |
| Self Test Quick Answer Key | 260 |

Chapter 4 Designing an Enterprise-Level Group

| | |
|--|------------|
| Policy Strategy | 261 |
| Introduction | 262 |
| Understanding Group Policy Preferences | 262 |
| ADMX/ADML Files | 265 |
| Understanding Group Policy Objects | 268 |
| Deciding Which Domain Controller Will Process GPOs | 270 |
| Group Policy Processing over Slow Links | 273 |
| Group Policy Processing over Remote Access Connections | 275 |
| Group Policy Background Refresh Interval | 275 |
| Backing Up and Restoring GPOs | 276 |
| User Policies | 279 |
| Software Installation | 280 |
| Security Settings | 281 |
| Folder Redirection Settings | 282 |
| Logon and Logoff Scripts | 284 |
| Administrative Templates | 286 |
| Computer Policies | 287 |
| Software Installation | 288 |
| Restricted Groups | 289 |
| Windows Firewall with Advanced Security | 290 |
| Policy-Based Quality of Service | 291 |
| Startup and Shutdown Scripts | 293 |
| Administrative Templates | 294 |
| GPO Templates | 295 |
| Starter GPOs | 295 |
| Linking GPOs to Active Directory Objects | 296 |
| Linking GPOs | 296 |
| GPO Conflicts | 297 |

| | |
|---|------------|
| RSoP | 300 |
| Managing Group Policy with Windows PowerShell | 303 |
| OU Hierarchy | 306 |
| Understanding Group Policy Hierarchy and Scope Filtering | 307 |
| Understanding Group Policy Hierarchies | 307 |
| Understanding Scope Filtering | 308 |
| Scope Filtering: Permissions | 308 |
| Scope Filtering: WMI Filters | 310 |
| Controlling Device Installation | 312 |
| Controlling Device Installation by Computer | 312 |
| Allowing/Preventing Installation of Devices Using Drivers | |
| That Match These Device Setup Classes | 313 |
| Display a Custom Message When Installation Is Prevented by | |
| Policy (Balloon Text/Title) | 313 |
| Allowing/Preventing Installation of Devices That Match | |
| Any of These Device IDs | 313 |
| Preventing Installation of Removable Devices | 314 |
| Preventing Installation of Devices Not Described by Any | |
| Other Policy Setting | 314 |
| Controlling Device Installation by User | 314 |
| Summary of Exam Objectives | 315 |
| Exam Objectives Fast Track | 315 |
| Exam Objectives Frequently Asked Questions | 318 |
| Self Test | 320 |
| Self Test Quick Answer Key | 325 |
| Chapter 5 Designing Identity and Access Management | 327 |
| Introduction | 328 |
| Planning for Migration, Upgrades, and Restructuring | 329 |
| Knowing When to Migrate or Upgrade | 329 |
| Backward Compatibility | 330 |
| Object Migration | 330 |
| The Object Global Unique Identifier in Active Directory | 331 |
| The Effect of an Upgrade or a Restructuring on | |
| SIDs and GUIDs | 332 |
| Leveraging SID History to Maintain Access to Resources | 333 |
| Using Active Directory Migration Tool to Restructure | |
| Domains | 334 |
| Maintaining User Passwords During a Restructure | 337 |
| Migrating Users and Groups | 339 |

| | |
|--|------------|
| Migrating Computer Accounts | 346 |
| Upgrading Your Active Directory Domain or Forest | 348 |
| Installing Windows Server 2008 Domain Controllers into an Existing Forest | 350 |
| Migration Planning | 352 |
| Knowing When to Restructure | 353 |
| Intra-Forest Domain Restructure | 354 |
| Intra-Forest Upgrade and Restructure | 357 |
| Cross-Forest Authentication | 359 |
| Implementation Planning | 360 |
| Planning for Interoperability | 360 |
| Interorganizational Strategies | 361 |
| Active Directory Federation Services | 361 |
| What Is Federation? | 362 |
| Why and When to Use Federation | 362 |
| Prerequisites for ADFS | 364 |
| Configuring ADFS | 364 |
| Application Authorization Interoperability | 376 |
| Using Active Directory Lightweight Directory Services to Provide Authentication and Authorization to Extranet Users | 376 |
| When to Use AD LDS | 377 |
| Changes from Active Directory Application Mode (ADAM) | 377 |
| Configuring AD LDS | 378 |
| Working with AD LDS | 381 |
| Cross-Platform Interoperability | 383 |
| File System Paths and Permissions on Unix Systems | 383 |
| Authentication on Unix Systems | 384 |
| Network Information System | 384 |
| NIS+ | 385 |
| Network File System (NFS) | 388 |
| Summary of Exam Objectives | 395 |
| Exam Objectives Fast Track | 397 |
| Exam Objectives Frequently Asked Questions | 399 |
| Self Test | 401 |
| Self Test Quick Answer Key | 404 |
| Chapter 6 Designing a Branch Office Deployment | 405 |
| Introduction | 406 |
| The Branch Office Challenge | 406 |
| Network Bandwidth | 406 |

| | |
|--|-----|
| Security..... | 406 |
| Backup and Restore..... | 407 |
| Hub-and-Spoke Topology | 408 |
| Developing an Authentication Strategy | 409 |
| Centralized Account Administration | 409 |
| Single Sign-on | 409 |
| Kerberos Authentication | 410 |
| Password Policies | 410 |
| When to Place a Domain Controller in a Remote Office..... | 411 |
| Number of Group Policies | 411 |
| Logon Scripts | 411 |
| User Population..... | 411 |
| Domain Controller Physical Security | 412 |
| On-Site Technical Expertise Availability | 412 |
| Authentication Availability | 412 |
| WAN Link Speed and Bandwidth Utilization | 412 |
| Bandwidth and Network Traffic Considerations..... | 412 |
| Placing a Global Catalog Server in a Remote Office | 414 |
| Universal Group Membership Caching..... | 415 |
| Full Domain Controller vs. Read-Only Domain Controller | 416 |
| Using BitLocker..... | 417 |
| Trusted Platform Modules..... | 417 |
| A Practical Example..... | 418 |
| Introduction to BitLocker | 418 |
| Full Volume Encryption..... | 419 |
| Startup Process Integrity Verification..... | 419 |
| Recovery Mechanisms | 420 |
| Remote Administration | 421 |
| Secure Decommissioning..... | 421 |
| BitLocker Architecture | 422 |
| Keys Used for Volume Encryption | 423 |
| Hardware Upgrades on BitLocker-Protected Systems..... | 424 |
| BitLocker Authentication Modes | 424 |
| TPM Only | 425 |
| TPM with PIN Authentication | 425 |
| TPM with Startup Key Authentication | 425 |
| Startup Key-Only | 426 |
| When to Use BitLocker on a Windows 2008 Server | 426 |

| | |
|--|-----|
| Support for Multifactor Authentication on Windows Server 2008 | 426 |
| PIN Authentication | 427 |
| Startup Key Authentication | 427 |
| Enabling BitLocker | 427 |
| Partitioning Disks for BitLocker Usage | 427 |
| Installing the BitLocker on Windows Server 2008 | 429 |
| Turning on BitLocker | 431 |
| Enable BitLocker Support for TPM-less Operation | 434 |
| Turning on BitLocker on Systems without a TPM | 435 |
| Administration of BitLocker | 437 |
| Using Group Policy with BitLocker | 437 |
| Storing BitLocker and TPM Recovery Information in Active Directory | 439 |
| Storage of BitLocker Recovery Information in Active Directory | 440 |
| Storage of TPM Information in Active Directory | 441 |
| Prerequisites | 441 |
| Extending the Schema | 442 |
| Setting Required Permissions for Backing Up TPM Passwords | 444 |
| Configuring Group Policy to Enable BitLocker and TPM Backup to Active Directory | 444 |
| Recovering Data | 445 |
| Disabling BitLocker | 447 |
| Configuring Read-Only Domain Controllers | 447 |
| Purpose | 448 |
| Features | 448 |
| Credential Caching | 449 |
| Password Changes on an RODC? | 450 |
| RODCs and Kerberos Ticket Account | 450 |
| Read-Only Domain Name System | 452 |
| Installing an RODC | 452 |
| Installation of an RODC | 454 |
| Prestaging RODC Computer Accounts | 457 |
| Full Server Installation vs. Server Core Installation | 460 |
| Configuring an RODC | 464 |
| Examining Cached Credentials | 468 |
| To Export a List of Cached Accounts | 469 |

| | |
|---|------------|
| Where Is a Password Replication Policy Stored? | 469 |
| Designing Password Replication Policies | 470 |
| No Account Caching | 471 |
| Full Account Caching | 471 |
| Branch-specific Caching | 472 |
| Role Separation | 472 |
| Configuring Role Separation | 474 |
| Remote Administration | 474 |
| Remote Desktop for Administration | 475 |
| Remote Server Administration Tools | 475 |
| Telnet | 476 |
| Windows Remote Management (WinRM) | 477 |
| WinRM Listeners | 477 |
| Remote Management Using WinRM | 478 |
| Group Policy | 479 |
| Summary of Exam Objectives | 480 |
| Exam Objectives Fast Track | 483 |
| Exam Objectives Frequently Asked Questions | 484 |
| Self Test | 486 |
| Self Test Quick Answer Key | 489 |
| Chapter 7 Configuring Certificate Services and PKI | 491 |
| Introduction | 492 |
| What Is PKI? | 493 |
| The Function of the PKI | 495 |
| Components of PKI | 496 |
| How PKI Works | 498 |
| PKCS Standards | 500 |
| How Certificates Work | 506 |
| Public Key Functionality | 509 |
| Digital Signatures | 510 |
| Authentication | 511 |
| Secret Key Agreement via Public Key | 512 |
| Bulk Data Encryption without Prior Shared Secrets | 512 |
| User Certificates | 525 |
| Machine Certificates | 526 |
| Application Certificates | 526 |
| Analyzing Certificate Needs within the Organization | 526 |
| Working with Certificate Services | 527 |
| Configuring a Certificate Authority | 527 |

| | |
|---|------------|
| Certificate Authorities | 528 |
| Standard vs. Enterprise. | 528 |
| Root vs. Subordinate Certificate Authorities | 529 |
| Certificate Requests | 530 |
| Certificate Practice Statement | 535 |
| Key Recovery | 535 |
| Backup and Restore. | 535 |
| Assigning Roles. | 542 |
| Enrollments. | 542 |
| Revocation | 543 |
| Working with Templates. | 547 |
| General Properties | 549 |
| Request Handling | 551 |
| Cryptography. | 552 |
| Subject Name | 554 |
| Issuance Requirements | 555 |
| Security | 558 |
| Types of Templates | 559 |
| User Certificate Types | 559 |
| Computer Certificate Types | 560 |
| Other Certificate Types | 562 |
| Custom Certificate Templates. | 562 |
| Securing Permissions | 565 |
| Versioning | 566 |
| Key Recovery Agent. | 567 |
| Summary of Exam Objectives. | 569 |
| Exam Objectives Fast Track | 570 |
| Exam Objectives Frequently Asked Questions | 572 |
| Self Test. | 575 |
| Self Test Quick Answer Key | 578 |
| Chapter 8 Planning for Server Virtualization | 579 |
| Introduction | 580 |
| Understanding Virtualization. | 580 |
| Server Consolidation | 583 |
| Quality Assurance and Development Testing Environments. | 584 |
| Disaster Recovery. | 587 |
| Microkernelized vs. Monolithic Hypervisor. | 588 |
| Monolithic Hypervisor. | 588 |
| Microkernel Hypervisor. | 590 |

| | |
|---|------------|
| Detailed Architecture | 591 |
| Parent Partition | 593 |
| Child Partitions | 595 |
| Guest Operating Systems | 595 |
| Guest with Enlightened Operating System | 595 |
| Guest with Partially Enlightened Operating System. | 596 |
| Legacy Guest | 596 |
| Application Compatibility. | 596 |
| Microsoft Server Virtualization | 597 |
| Hyper-V | 600 |
| Configuration | 601 |
| Installing the Virtualization Role on Windows Server 2008. | 602 |
| Configuring Virtual Servers with Hyper-V | 614 |
| Server Core | 624 |
| Competition Comparison. | 626 |
| Server Placement | 628 |
| System Center Virtual Machine Manager 2007 | 630 |
| Virtual Machine Manager Administrator Console. | 632 |
| Windows PowerShell Command-Line Interface. | 634 |
| System Center Virtual Machine Manager | |
| Self Service Web Portal | 634 |
| Virtual Machine Manager Library | 635 |
| Migration Support Functionality. | 636 |
| Virtual Machine Creation Process Using SCVMM. | 637 |
| Managing Servers | 638 |
| Stand-Alone Virtualization Management Console. | 639 |
| Managing Applications | 640 |
| Managing VMWare. | 644 |
| Summary of Exam Objectives. | 646 |
| Exam Objectives Fast Track | 647 |
| Exam Objectives Frequently Asked Questions | 651 |
| Self Test. | 654 |
| Self Test Quick Answer Key | 657 |
| Chapter 9 Planning for Business Continuity and High Availability | 659 |
| Introduction | 660 |
| Planning for Storage Requirements. | 661 |
| Self Healing NTFS. | 662 |
| Multipath I/O (MPIO). | 663 |

| | |
|---|-----|
| Data Management | 664 |
| Share and Storage Management Console. | 664 |
| Storage Explorer | 665 |
| Storage Manager for SANs Console | 666 |
| Data Security | 667 |
| Group Policy Control over Removable Media | 667 |
| BitLocker Drive Encryption. | 668 |
| BitLocker Volume Recovery | 670 |
| BitLocker Management Options | 670 |
| Using BitLocker for the Safe Decommissioning of Hardware | 671 |
| Data Collaboration. | 672 |
| Planning for High Availability | 677 |
| Failover Clustering | 677 |
| Architectural Details of Windows 2008 Failover Clustering | 678 |
| Multi-Site Clusters. | 694 |
| Service Redundancy. | 695 |
| Service Availability | 697 |
| Data Accessibility and Redundancy | 697 |
| Failover Clustering. | 698 |
| Prerequisites | 698 |
| Distributed File System | 699 |
| Virtualization and High Availability | 700 |
| Planning for Backup and Recovery | 701 |
| Data Recovery Strategies | 716 |
| Server Recovery. | 717 |
| WinRE Recovery Environment Bare Metal Restore | 718 |
| Command Line Bare Metal Restore | 719 |
| Recovering Directory Services | 719 |
| Backup Methods for Directory Services | 719 |
| Backup Types for Directory Services | 720 |
| Recovery Methods for Directory Services. | 720 |
| Directory Services Restore Mode Recovery | 720 |
| Non-Authoritative Restore | 721 |
| Authoritative Restore | 723 |
| Object Level Recovery. | 723 |
| Summary of Exam Objectives. | 731 |
| Exam Objectives Fast Track | 731 |
| Exam Objectives Frequently Asked Questions | 736 |

| | |
|--|------------|
| Self Test | 739 |
| Self Test Quick Answer Key | 742 |
| Chapter 10 Software Updates and Compliance Management | 743 |
| Introduction | 744 |
| Value Proposition | 745 |
| The Compliance Picture | 746 |
| Patch Management | 747 |
| OS Level Patch Management | 748 |
| Windows Server Update Services | 749 |
| System Requirements | 750 |
| Types of Patches | 751 |
| Comparison to Microsoft Update | 753 |
| Implementing WSUS | 754 |
| Designing a WSUS Infrastructure | 754 |
| Small Enterprise (1–100 Workstations) | 754 |
| Branch Office Deployment | 755 |
| Large Enterprises | 756 |
| Deploying to Client Computers | 768 |
| Application Patching | 774 |
| Security Baselines | 774 |
| What Is a Baseline? | 775 |
| Using the GPO Accelerator Tool | 775 |
| Requirements | 777 |
| Supported Security Baselines | 777 |
| Using the Baseline Security Analyzer | 783 |
| Comparison to Microsoft Update | 783 |
| Implementing MBSA | 784 |
| Analyzing MBSA Results | 786 |
| System Health Models | 788 |
| What Is a System Health Model? | 788 |
| Developing a Health Model | 789 |
| Summary of Exam Objectives | 790 |
| Exam Objectives Fast Track | 790 |
| Exam Objectives Frequently Asked Questions | 794 |
| Self Test | 797 |
| Self Test Quick Answer Key | 802 |
| Appendix Self Test Appendix | 803 |
| Chapter 1: Name Resolution and IP Addressing | 804 |
| Chapter 2: Designing a Network Access Strategy | 809 |

xxvi Contents

| | |
|---|------------|
| Chapter 3: Active Directory Forests and Domains | 814 |
| Chapter 4: Designing an Enterprise-Level Group Policy Strategy | 822 |
| Chapter 5: Designing Identity and Access Management | 829 |
| Chapter 6: Designing a Branch Office Deployment | 834 |
| Chapter 7: Developing a Public Key Infrastructure. | 839 |
| Chapter 8: Planning for Server Virtualization | 845 |
| Chapter 9: Planning for Business Continuity and High Availability | 850 |
| Chapter 10: Software Updates and Compliance Management. | 856 |
| Index | 865 |

Foreword

This book's primary goal is to help you prepare to take and pass Microsoft's exam number 70-647, *Windows Server 2008 Enterprise Administrator*. Our secondary purpose in writing this book is to provide exam candidates with knowledge and skills that go beyond the minimum requirements for passing the exam, and help to prepare them to work in the real world of Microsoft computer networking.

What Is Professional Series Exam 70-647?

Professional Series Exam 70-647 is the final requirement for those pursuing *Microsoft Certified Information Technology Professional (MCITP): Enterprise Administrator* certification for Windows Server 2008. The Enterprise Administrator is responsible for the entire IT infrastructure and architecture for an organization, and makes midrange and long-range strategic technology decisions based on business goals. Candidates for this certification are IT professionals who seek a leadership role in Windows infrastructure design in a current or future job role, in which they work with Windows Server 2008.

However, not everyone who takes Exam 70-647 will have practical experience in IT management. Many people will take this exam after classroom instruction or self-study as an entry into the networking field. Many of those who do have job experience in IT will not have had the opportunity to work with all of the technologies or be involved with the infrastructure and architecture issues covered by the exam. In this book, our goal is to provide background information that will help

you to understand the concepts and procedures described even if you don't have the requisite experience, while keeping our focus on the exam objectives.

Exam 70-647 covers the complex concepts involved with administering a network environment that is built around Microsoft's Windows Server 2008. The exam includes the following task-oriented objectives:

- **Planning Network and Application Services:** This includes planning for name resolution and IP addressing, designing for network access, planning for application delivery, and planning for terminal services.
- **Designing Core Identity and Access Management Components:** This includes designing Active Directory forests and domains, designing the Active Directory physical topology, designing the Active Directory administrative model, and designing the enterprise-level group policy strategy.
- **Designing Support Identity and Access Management Components:** This includes planning for domain or forest migration, upgrade, and restructuring; designing the branch office deployment; designing and implementing public key infrastructure; and planning for interoperability.
- **Designing for Business Continuity and Data Availability:** This includes planning for business continuity, designing for software updates and compliance management, designing the operating system virtualization strategy, and designing for data management and data access.

NOTE

In this book, we have tried to follow Microsoft's exam objectives as closely as possible. However, we have rearranged the order of some topics for a better flow, and included background material to help you understand the concepts and procedures that are included in the objectives.

Path to MCTS/MCITP/MS Certified Architect

Microsoft certification is recognized throughout the IT industry as a way to demonstrate mastery of basic concepts and skills required to perform the tasks involved in implementing and maintaining Windows-based networks. The certification program is constantly evaluated and improved, and the nature of information technology is changing rapidly. Consequently, requirements and specifications for certification can also change rapidly. This book is based on the exam objectives as stated by Microsoft at the time of writing; however, Microsoft reserves the right to make changes to the objectives and to the exam itself at any time. Exam candidates should regularly visit the Certification and Training Web site at www.microsoft.com/learning/mcp/default.mspx for the most updated information on each Microsoft exam.

Microsoft currently offers three basic levels of certification on the technology level, professional level, and architect level:

- **Technology Series** This level of certification is the most basic, and it includes the **Microsoft Certified Technology Specialist (MCTS)** certification. The MCTS certification is focused on one particular Microsoft technology. There are 19 MCTS exams at the time of this writing. Each MCTS certification consists of one to three exams, does not include job-role skills, and will be retired when the technology is retired. Microsoft Certified Technology Specialists will be proficient in implementing, building, troubleshooting, and debugging a specific Microsoft technology.
- **Professional Series** This is the second level of Microsoft certification, and it includes the **Microsoft Certified Information Technology Professional (MCITP)** and **Microsoft Certified Professional Developer (MCPD)** certifications. These certifications consist of one to three exams, have prerequisites from the Technology Series, focus on a specific job role, and require an exam refresh to remain current. The MCITP certification offers nine separate tracks as of the time of this writing. There are two Windows Server 2008 tracks, Server Administrator and Enterprise Administrator. To achieve the Server Administrator MCITP for Windows Server 2008, you must successfully complete one Technology Series exam and one Professional Series exam.

To achieve the Enterprise Administrator MCITP for Windows Server 2008, you must successfully complete four Technology Series exams and one Professional Series exam.

- **Architect Series** This is the highest level of Microsoft certification, and it requires the candidate to have at least 10 years' industry experience. Candidates must pass a rigorous review by a review board of existing architects, and they must work with an architect mentor for a period of time before taking the exam.

NOTE

Those who already hold the MCSA or MCSE in Windows 2003 can upgrade their certifications to MCITP Server Administrator by passing one upgrade exam and one Professional Series exam. Those who already hold the MCSA or MCSE in Windows 2003 can upgrade their certifications to MCITP Enterprise Administrator by passing one upgrade exam, two Technology Series exams, and one Professional Series exam.

Prerequisites and Preparation

Although you may take the required exams for *MCITP: Enterprise Administrator* certification in any order, successful completion of the following MCTS exams is required for certification, in addition to Professional Series Exam 70-647:

- 70-620 *Configuring Microsoft Windows Vista Client* **or** 70-624 *Deploying and Maintaining Windows Vista Client and 2007 Microsoft Office System Desktops*
- 70-640 *Configuring Windows Server 2008 Active Directory*
- 70-642 *Configuring Windows Server 2008 Network Infrastructure*
- 70-643 *Configuring Windows Server 2008 Applications Platform*

NOTE

Those who already hold the MCSA in Windows Server 2003 can upgrade their certifications to MCITP Enterprise Administrator by substituting exam 70-648 for exams 70-640 and 70-642 above. Those who already hold the MCSE in Windows Server 2003 can upgrade their certifications to MCITP Enterprise Administrator by substituting exam 70-649 for exams 70-640, 70-642, and 70-643 above.

Preparation for this exam should include the following:

- Visit the Web site at www.microsoft.com/learning/exams/70-647.mspx to review the updated exam objectives.
- Work your way through this book, studying the material thoroughly and marking any items you don't understand.
- Answer all practice exam questions at the end of each chapter.
- Complete all hands-on exercises in each chapter.
- Review any topics that you don't thoroughly understand.
- Consult Microsoft online resources such as TechNet (www.microsoft.com/technet/), white papers on the Microsoft Web site, and so forth, for better understanding of difficult topics.
- Participate in Microsoft's product-specific and training and certification newsgroups if you have specific questions that you still need answered.
- Take one or more practice exams, such as the one included on the Syngress/Elsevier certification Web site at www.syngress.com/certification/70647.

Exam Day Experience

Taking the exam is a relatively straightforward process. Prometric testing centers administer the Microsoft 70-647 exam. You can register for, reschedule or cancel an exam through the Prometric Web site at www.register.prometric.com. You'll find listings of testing center locations on these sites. Accommodations are made for those with disabilities; contact the individual testing center for more information.

Exam price varies depending on the country in which you take the exam.

Exam Format

Exams are timed. At the end of the exam, you will find out your score and whether you passed or failed. You will not be allowed to take any notes or other written materials with you into the exam room. You will be provided with a pencil and paper, however, for making notes during the exam or doing calculations.

In addition to the traditional multiple-choice questions and the select-and-drag, simulation, and case study questions, you might see some or all of the following types of questions:

- *Hot area* questions, in which you are asked to select an element or elements in a graphic to indicate the correct answer. You click an element to select or deselect it.
- *Active screen* questions, in which you change elements in a dialog box (for example, by dragging the appropriate text element into a text box or selecting an option button or checkbox in a dialog box).
- *Drag-and-drop* questions, in which you arrange various elements in a target area.

Test-Taking Tips

Different people work best using different methods. However, there are some common methods of preparation and approach to the exam that are helpful to many test-takers. In this section, we provide some tips that other exam candidates have found useful in preparing for and actually taking the exam.

- Exam preparation begins before exam day. Ensure that you know the concepts and terms well and feel confident about each of the exam objectives. Many test-takers find it helpful to make flash cards or review notes to study on the way to the testing center. A sheet listing acronyms and abbreviations can be helpful, as the number of acronyms (and the similarity of different acronyms) when studying IT topics can be overwhelming. The process of writing the material down, rather than just reading it, will help to reinforce your knowledge.
- Many test-takers find it especially helpful to take practice exams that are available on the Internet and with books such as this one. Taking the practice exams can help you become used to the computerized exam-taking experience, and the practice exams can also be used as

a learning tool. The best practice tests include detailed explanations of why the correct answer is correct and why the incorrect answers are wrong.

- When preparing and studying, you should try to identify the main points of each objective section. Set aside enough time to focus on the material and lodge it into your memory. On the day of the exam, you should be at the point where you don't have to learn any new facts or concepts, but need simply to review the information already learned.
- The value of hands-on experience cannot be stressed enough. Exam questions are based on test-writers' experiences in the field. Working with the products on a regular basis—whether in your job environment or in a test network that you've set up at home—will make you much more comfortable with these questions.
- Know your own learning style and use study methods that take advantage of it. If you're primarily a visual learner, reading, making diagrams, watching video files on CD, etc., may be your best study methods. If you're primarily auditory, listening to classroom lectures, using audiotapes that you can play in the car as you drive, and repeating key concepts to yourself aloud may be more effective. If you're a kinesthetic learner, you'll need to actually *do* the exercises, implement the security measures on your own systems, and otherwise perform hands-on tasks to best absorb the information. Most of us can learn from all of these methods, but have a primary style that works best for us.
- Although it may seem obvious, many exam-takers ignore the physical aspects of exam preparation. You are likely to score better if you've had sufficient sleep the night before the exam, and if you are not hungry, thirsty, hot/cold, or otherwise distracted by physical discomfort. Eat prior to going to the testing center (but don't indulge in a huge meal that will leave you uncomfortable), stay away from alcohol for 24 hours prior to the test, and dress appropriately for the temperature in the testing center (if you don't know how hot/cold the testing environment tends to be, you may want to wear light clothes with a sweater or jacket that can be taken off).
- Before you go to the testing center to take the exam, be sure to allow time to arrive on time, take care of any physical needs, and step back to take a deep breath and relax. Try to arrive slightly early, but not so far

in advance that you spend a lot of time worrying and getting nervous about the testing process. You may want to do a quick last-minute review of notes, but don't try to "cram" everything the morning of the exam. Many test-takers find it helpful to take a short walk or do a few calisthenics shortly before the exam to get oxygen flowing to the brain.

- Before beginning to answer questions, use the pencil and paper provided to you to write down terms, concepts, and other items that you think you may have difficulty remembering as the exam goes on. Then you can refer back to these notes as you progress through the test. You won't have to worry about forgetting the concepts and terms you have trouble with later in the exam.
- Sometimes the information in a question will remind you of another concept or term that you might need in a later question. Use your pen and paper to make note of this in case it comes up later on the exam.
- It is often easier to discern the answer to scenario questions if you can visualize the situation. Use your pen and paper to draw a diagram of the network that is described to help you see the relationships between devices, IP addressing schemes, and so forth.
- When appropriate, review the answers you weren't sure of. However, you should change your answer only if you're sure that your original answer was incorrect. Experience has shown that more often than not, when test-takers start second-guessing their answers, they end up changing correct answers to the incorrect. Don't "read into" the question (that is, don't fill in or assume information that isn't there); this is a frequent cause of incorrect responses.
- As you go through this book, pay special attention to the Exam Warnings, as these highlight concepts that are likely to be tested. You may find it useful to go through and copy these into a notebook (remembering that writing something down reinforces your ability to remember it) and/or go through and review the Exam Warnings in each chapter just prior to taking the exam.
- Use as many little mnemonic tricks as possible to help you remember facts and concepts. For example, to remember which of the two IPsec

protocols (AH and ESP) encrypts data for confidentiality, you can associate the “E” in encryption with the “E” in ESP.

Pedagogical Elements

In this book, you’ll find a number of different types of sidebars and other elements designed to supplement the main text. These include the following:

- **Exam Warning** These sidebars focus on specific elements on which the reader needs to focus in order to pass the exam (for example, “Be sure you know the difference between symmetric and asymmetric encryption”).
- **Test Day Tip** These sidebars are short tips that will help you in organizing and remembering information for the exam (for example, “When you are preparing for the exam on test day, it may be helpful to have a sheet with definitions of these abbreviations and acronyms handy for a quick last-minute review”).
- **Configuring & Implementing** These sidebars contain background information that goes beyond what you need to know from the exam, but provide a “deep” foundation for understanding the concepts discussed in the text.
- **New & Noteworthy** These sidebars point out changes in Windows Server 2008 from Windows Server 2003, as they will apply to readers taking the exam. These may be elements that users of Windows Server 2003 would be very familiar with that have changed significantly in Windows Server 2008 or totally new features that they would not be familiar with at all.
- **Head of the Class** These sidebars are discussions of concepts and facts as they might be presented in the classroom, regarding issues and questions that most commonly are raised by students during study of a particular topic.

Each chapter of the book also includes hands-on exercises in planning and configuring the features discussed. It is essential that you read through and, if possible, perform the steps of these exercises to familiarize yourself with the processes they cover.

You will find a number of helpful elements at the end of each chapter. For example, each chapter contains a *Summary of Exam Objectives* that ties the topics discussed in that chapter to the published objectives. Each chapter also contains an *Exam Objectives Fast Track*, which boils all exam objectives down to manageable summaries that are perfect for last-minute review. *The Exam Objectives Frequently Asked Questions* answers those questions that most often arise from readers and students regarding the topics covered in the chapter. Finally, in the *Self Test* section, you will find a set of practice questions written in a multiple-choice format that will assist you in your exam preparation. These questions are designed to assess your mastery of the exam objectives and provide thorough remediation, as opposed to simulating the variety of question formats you may encounter in the actual exam. You can use the *Self Test Quick Answer Key* that follows the *Self Test* questions to quickly determine what information you need to review again. The *Self Test Appendix* at the end of the book provides detailed explanations of both the correct and incorrect answers.

Additional Resources

There are two other important exam preparation tools included with this study guide. One is the CD included in the back of this book. The other is the concept review test available from our Web site.

- **A CD that provides book content in multiple electronic formats for exam-day review** Review major concepts, test day tips, and exam warnings in PDF, PPT, MP3, and HTML formats. Here, you'll cut through all of the noise to prepare you for exactly what to expect when you take the exam for the first time. You will want to use this CD just before you head out to the testing center!
- **Web-based practice exams** Just visit us at www.syngress.com/certification to access a complete Windows Server 2008 concept multiple-choice review. These remediation tools are written to test you on all of the published certification objectives. The exam runs in both "live" and "practice" mode. Use "live" mode first to get an accurate gauge of your knowledge and skills, and then use practice mode to launch an extensive review of the questions that gave you trouble.

Chapter 1

MCITP Exam 647

Name Resolution and IP Addressing

Exam objectives in this chapter:

- Windows 2008 Name Resolution Methods
- Domain Name System
- DNS Server Implementation
- Windows Internet Naming Service (WINS)
- IPv4 and IPv6 Coexistence

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

Windows computers across organizations communicate with each other through the use of IP addresses. Computers use the TCP/IP protocol suite for the communication. Thus, it is important to create the proper IP addressing scheme for host identification and effective computer-to-computer communication.

IP addressing works great for intercomputer communication, but it does not work as well for humans. Imagine trying to remember the IP addresses of all the computers you access. Not only would it be extremely difficult, it would be a painful task to work with computers. Therefore, computers are assigned names, which are much easier to remember than IP addresses.

With computer names, you can just type the name of the computer to access it, instead of its IP address. However, accessing the computer by name does not happen automatically. A name resolution process runs in the background, which translates a computer name to its IP address. In this chapter, we will look into how the computer names are associated with IP addresses and what services are used to resolve the computer names. Without the proper name resolution, communication between the computers in an organization will simply not exist.

Windows 2008 Name Resolution Methods

This chapter looks into what services are used in Windows 2008 for name resolution, as well as what factors play roles in the Windows 2008 Name Resolution.

The following two systems are used within the Windows environment for name resolution:

- Domain Name System (DNS)
- Windows Internet Naming Service (WINS)

Developing a Naming Strategy

It is important for any organization to create a proper naming strategy for their Windows environment. This will give them the ability to properly identify various computers within their environment. Therefore, much thought must go into defining an effective naming scheme.

Assigning names randomly can create difficulties in recognizing the host, as well as cause problems in some troubleshooting scenarios. A well thought out and

well-defined naming scheme is even more important for large organizations that have hundreds or thousands of computer hosts located at various physical locations. A proper record should always be kept of all the host names assigned. When a problem occurs, the proper naming scheme will also help identify any unauthorized and unrecognized machines in the environment or identify a machine compromised by a virus or malware.

Windows environments, beginning with Windows 2000 Server, primarily use DNS for name resolution; however, some legacy Windows clients and applications may be using NetBIOS names. Many organizations have moved to DNS because of the introduction of Active Directory, but some find they cannot totally remove NetBIOS from their environment due to some legacy server or application that depends on it (such as Microsoft File and Printer Sharing). Also, it should be noted that host names in NetBIOS are limited to 15 characters, while host names in DNS can go up to 63 characters, and 255 characters FQDN, including the trailing dots.

A proper naming scheme provides guidance for administrators on how to assign names for servers, desktops, laptops, printers, and various other hosts, taking into account their role, locations, business units, and so on.

Comparing Name Resolution Procedures

Within these two methods of name resolution—DNS and NetBIOS—Windows Server 2008 networks provide the following set of mechanisms to resolve computer names:

The DNS name resolution method includes the following:

- Name lookup in the local DNS client cache, also called the *local resolver*. Names can be cached from previous queries. They can also be loaded from the HOSTS file found in the %systemroot%\System32\Drivers\Etc folder.
- Query on a DNS server.

The NetBIOS name resolution method includes the following:

- Name lookup in the local NetBIOS name cache.
- Query on WINS server.
- Local network query through NetBIOS broadcasts.
- Name lookup in the LMHOST file, located in the WINDOWS\System32\Drivers\Etc folder.

Table 1.1 compares the basic features of DNS host names and NetBIOS computer names.

Table 1.1 Comparison between DNS Names and NetBIOS Names

| Type | Hierarchical | Flat |
|------------------------|---|--|
| Character restrictions | A–Z, a–z, 0–9, and the hyphen (-); period (.) has special reserved symbols: meaning | Unicode characters, numbers, white space, ! @ # \$ % ^ & ') (. - _ { } ~ |
| Maximum length | 63 bytes per label; 255 bytes per FQDN | 15 characters |
| Name service | DNS HOST File | WINS NetBIOS broadcasts LMHOST File |

Internal Names

Internal names are private company namespaces. Internal namespaces are created for a company's own internal use and are not regulated by the Internet Corporation for Assigned Names and Numbers (ICANN). Within private domain names, you can create or remove the subdomain names as needed. For example, you could create .lab for your internal lab network or .local for your internal company's network. This way you can keep the internal network separate from the public Internet. However, you would have to use a Network Address Translation (NAT) server or a proxy server to have your internal network communicate with the Internet. Private names are not resolved or addressed directly by the Internet.

External Names

External names are public names. Public names are accessible via the Internet. They are created for public use and are regulated by ICANN. They must be registered with a domain registration service. External names cannot be used publicly without them first being reserved and authorized by domain name registrars, such as Network Solutions, which charge a fee for this service.

We will discuss strategies in implementing internal and external name resolution design later in DNS section.

Domain Name System

Domain Name System (DNS) is a network of distributed databases that translates computer names to their corresponding IP addresses. Before we look further into DNS, let's review what is meant by "host name," "domain name," and "fully qualified domain name."

Host Names

A host name is basically a computer name with one distinction. DNS has a record of the host name in its database as well as the corresponding IP address. The record is known as the host record. Host names are usually assigned by administrators. They can also be assigned by various other authorized organization members. Host names can have a maximum length of 255 characters. However, host records in DNS are limited to a maximum length of 255 characters, which includes the parent domain names and the "dots" in between and at the end.

Domain Names

A network in DNS is identified by a domain name. A domain name follows a specific hierarchical naming system. Name components or various levels within a domain are separated by dots (.)

The top level in the hierarchy, which includes the top-level domains, consists of root domains. Root domains identify the type of networks that are part of their domain. For example, .gov is for US Government domains, .edu for educational domains, and .com for commercial domains (see Table 1.2). Some of the root domains are also organized geographically, such as .ca for Canada.

Table 1.2 A Sampling of the Top-Level Domain Names

| Domain | Purpose |
|--------|---|
| .aero | For aerospace firms, including airlines |
| .biz | For businesses, extends the .com area |
| .com | For commercial organizations |
| .coop | For business cooperatives |
| .edu | For educational institutions |

Continued

Table 1.2 Continued. A Sampling of the Top-Level Domain Names

| Domain | Purpose |
|---------|---|
| .gov | For U.S. government agencies |
| .info | For information sources |
| .int | For organizations established by international treaties |
| .mil | For U.S. military departments and agencies |
| .museum | For museums |
| .name | For use by individuals |
| .net | For use by network providers |
| .org | For use by organizations, such as those that are nongovernmental or nonprofit |
| .pro | For professional groups such as doctors and lawyers |

Domains in the second level of the hierarchy are called parent domains. Parent domains are basically the primary domain names of the organizations. For Example, Microsoft Corporation's domain name is Microsoft.com. The domain name Microsoft.com identifies a specific network in the .com domain. Parent names cannot be used publicly without having them first be reserved and authorized by a domain name registrar, such as Network Solutions (which, again, charges a fee for the service).

All additional levels within the hierarchy are either individual hosts or further levels within the organization's domain. These subsequent levels are called child domains. For example, Microsoft's various divisions (such as sales, support, and technet) are named sales.microsoft.com, support.microsoft.com, and technet.microsoft.com, respectively.

Fully Qualified Domain Name (FQDN)

A fully qualified domain name (FQDN) combines the host name and the corresponding domain names to identify the host. All hosts within a TCP/IP network have a unique FQDN. For example, a host name can be server1, which is part of the support.microsoft.com domain, so the resulting “fully qualified domain name” would be server1.support.microsoft.com.

DNS is a client/server protocol, which means there is a client component and server component in any working DNS system. As in a client/server model, any

computer seeking DNS information is called a DNS client, while a computer responding to the information request is called the DNS Server.

New & Noteworthy...

DNS Enhancements in Windows Server 2008

Windows Server 2008 introduces many new enhancements in DNS Server service. Some of these improvements extend to the clients, such as the Windows Vista operating system. Overall, these have increased the performance of DNS servers, as well as the administration of these servers. The following list items include the major highlights:

- **Background Zone Loading** This feature in Windows Server 2008 enables the DNS server to respond to DNS queries as soon it starts up. In previous versions of Windows Server, zones had to be fully loaded before DNS Server could respond to DNS queries from clients. If the DNS client requests information for a host that has already been loaded in a zone, the DNS server will respond back with the information. If data is not loaded yet, it will read the requested data from Active Directory and update the record accordingly.
- **Full Support for IPv6** Windows Server 2008 provides full support for IPv6 addresses along with IPv4 addresses. The IP addresses are accepted in either format at the DNS console and at the command prompt using *dnscmd*. Recursive queries can be sent to IPv6 servers only. DNS servers can now return both IPv4 host (A) resource records and IPv6 host (AAAA) resource records in response to queries. IPv6 is a next-generation IP protocol. It increases the address space from 32 to 128 bits, providing for a virtually unlimited (for all intents and purposes) number of networks and systems. It also supports quality of service (QoS) parameters for real-time audio and video. Originally called “IP Next Generation” (IPng), IPv6 is expected to slowly replace IPv4, with the two existing side by side for many years.

Continued

- **Primary Read-Only Zone** In Windows Server 2008, there is a new type of domain controller called a read-only domain controller (RODC). RODC is a shadow copy of a domain controller; however, it is a read-only copy and cannot be modified. To support RODC, Windows Server 2008 running DNS server uses primary read-only zones.
- **GlobalNames Zone** The DNS Server service in Windows Server 2008 supports a zone called GlobalNames zone, which is used to hold single-label names similar to WINS server. The replication scope of this zone is the entire forest—meaning the zone data is replicated to all domain controllers in the forest. It can also span across forests within an organization to resolve the single-label names. It is used to provide single-label names for limited hosts and is not intended for all host registrations. Also dynamic updates are not supported.
- **Global Query Block List** Windows Server 2008 introduces a special and more secure mechanism for registrations through a dynamic DNS client.
- **LLMR** This new functionality is more on the client side at Windows Vista, in conjunction with Windows Server 2008. DNS clients running Windows Vista can use link-local multicast name resolution (LLMR) to resolve names on a local network when a DNS server is not available. This is also known as multicast DNS or mDNS.

Is DNS Required?

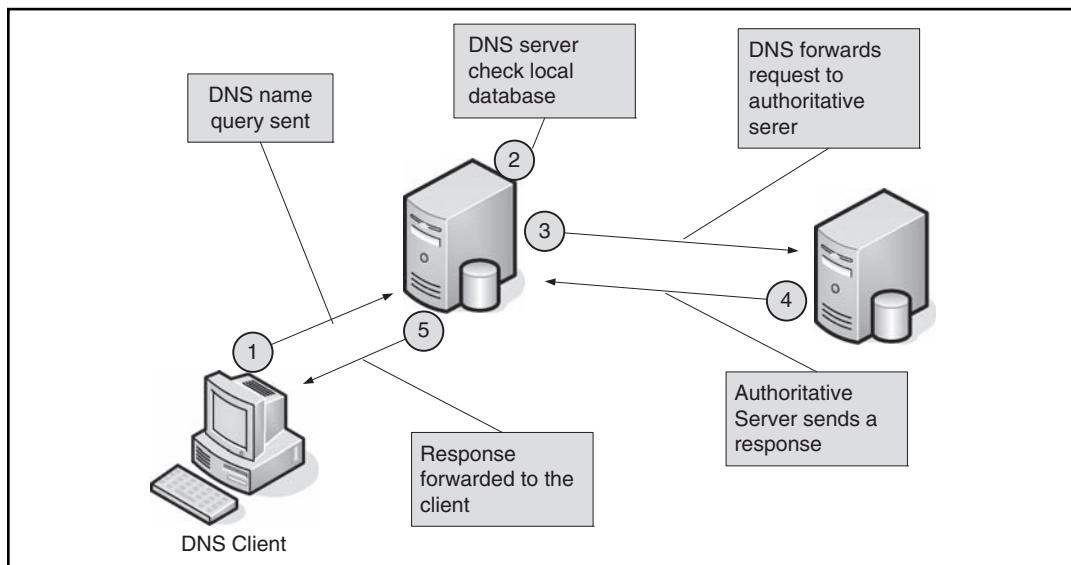
Not all network configurations require DNS Server in their environment. Many small networks can work without having DNS server installed within their network. However, typically, DNS is required in network environments with the following circumstances:

- **For Internet Access** DNS must be used to access the computers over the Internet.
- **For Windows 2000 Server domains and onward** For systems using Windows 2000, Windows 2003 or Windows 2008 Server domains, DNS must be installed and configured. DNS is required for Active Directory, and Active Directory and DNS are tightly integrated.

DNS Queries

A DNS query is made when a DNS client seeks information from a DNS server. The DNS server receiving the DNS query checks its local database to attempt to resolve it (see Figure 1.1). If there is no record in its database, the DNS server forwards the request to an authoritative DNS server.

Figure 1.1 Client Sending a DNS Query



Several types of queries are used in DNS, including forward lookup queries and reverse lookup queries. Each is briefly described next:

- **Forward lookup queries** These queries allow a DNS client to resolve host name to an IP address. The name query is initiated by a DNS client seeking the host address record for a specific host. The DNS server returns with the IP address of the requested host record if it is available. In case the host name is an alias of another host, the DNS server sends back both: the host address record of the alias (CNAME) and the host address record to which the alias points. For example, pinging server1.nsoftad.com resolves to its IP address 10.10.3.20.
- **Reverse lookup queries** These queries allow a DNS client to resolve an IP address to its corresponding host name. The name query is initiated by a

DNS client seeking a host name record for a specific IP address. The DNS server returns with the host name record of the requested IP address if it is available. This host name record in the return message is called the reverse address record (RTR). For example, pinging 10.10.3.20 resolves to its host name server1.nsoftad.com.

Each query message sent by a DNS client contains the following:

- A DNS domain name, stated as a fully qualified domain name (FQDN). If the FQDN is not provided by the client, the DNS client service will add the suffix to generate a FQDN.
- Query type specified.
- A special class for the DNS domain name. This class is always classified as the Internet class (IN) for the DNS client service.

The DNS Query Process

A DNS query can be resolved in many different ways. Generally, when a client initiates a DNS query to a DNS server, the DNS server will check its local database first. If there is no record in the local database of the DNS server, it forwards the information to other DNS servers. However, sometimes a DNS client resolves the query before seeking the information from the DNS server by looking into its own cache first.

Generally, the typical query process occurs in two parts:

- The client computer initiates a query and passes it on to the DNS client service for name resolution. DNS client service then tries to resolve the name locally from its cache.
- If the query cannot be resolved locally, it will be passed to a DNS server.

These parts are explained in more detail in the following.

Part 1: The Local Resolver

The DNS query process starts when a computer application uses a DNS domain name. In an example, a program on the computer, such as a Web browser, calls for www.microsoft.com. The request is passed to DNS client service which in turn looks at its locally cached information. This locally cached information is called the

DNS resolver cache. The query process ends here if the query can be resolved by the DNS resolver cache.

The local resolver cache obtains name information through two methods:

- If there is a Hosts file in place. When DNS service starts, all the host name to IP address mappings are loaded from the Hosts file to the local cache.
- Previous queries to the DNS server and host record information obtained by those queries. These responses are stored on the local cache for certain period of time.

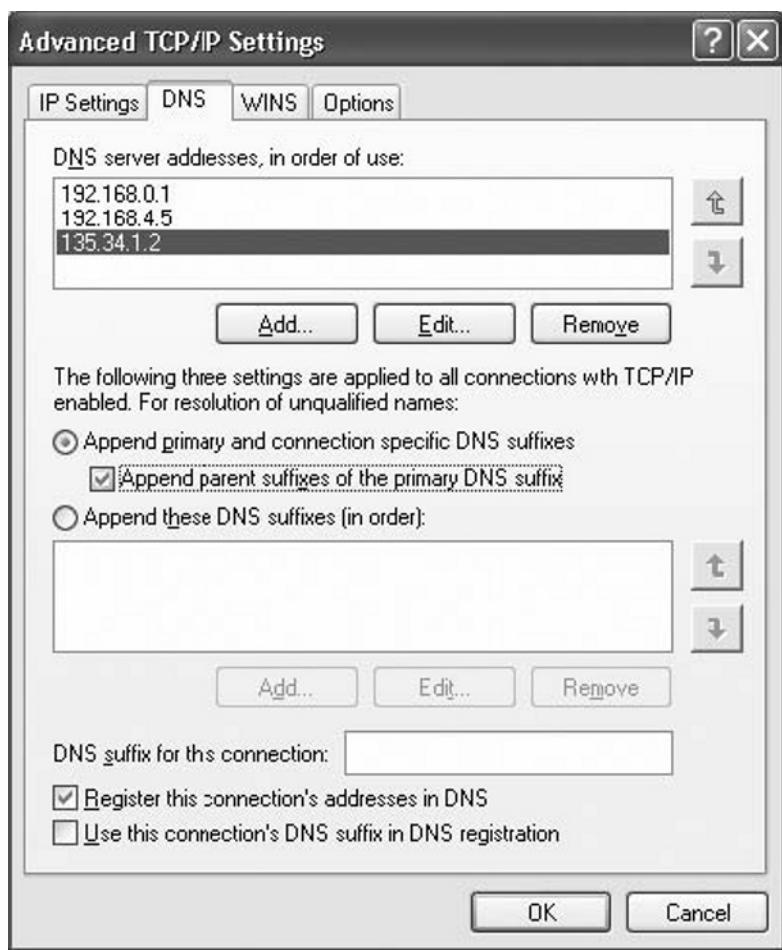
NOTE

This cache is cleared when the computer restarts. You can also manually clear the DNS resolver cache by opening a command prompt and typing `ipconfig /flushdns`.

The preceding example illustrates the default DNS query process. The DNS client is configured to initiate recursive queries to a server. If the query cannot be resolved by the local DNS resolver on the client, the client sends out only a single query to a DNS server. The called DNS server will then be responsible for answering the query. That DNS server will first look into its own records. The DNS server also checks its own cache for the requested host record. If there is no resolution locally at the DNS server, that DNS server will send out the query to other DNS servers. In turn, the sending DNS server becomes a DNS client at this point for this query.

Part 2: Querying a DNS Server

DNS servers have to be defined on the DNS client. They can be defined via the Dynamic Host Configuration Protocol (DHCP) server or manually. The defined list of DNS servers are listed in order of preference. They are defined in the client's Internet protocol properties, as shown in Figure 1.2. If the preferred DNS server is not available to respond, the client sends out the query to alternate DNS servers as defined in the list.

Figure 1.2 The DNS Preferred and Alternate Server List

After receiving a query, the DNS server checks to see if it can resolve that query authoritatively—which means based on the information in its locally configured zones. We will discuss zones later in the chapter. If the host name record exists on the locally configured zones (zones that are configured on the DNS server itself), the DNS server answers the query from the information.

If the query cannot be resolved by the DNS server from its zone configuration, the DNS server will check its local cache to see if the host record exists from previous queries. If the host record exists, the DNS server responds with the information. The query process stops here if the match is found and the server responds.

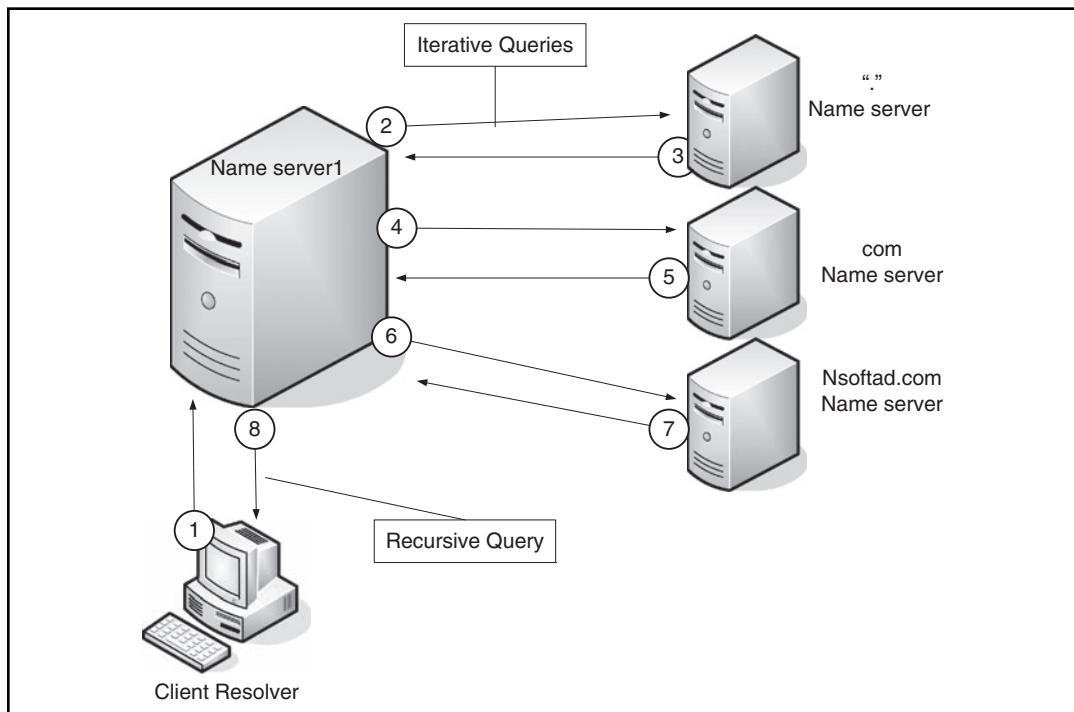
If a query cannot be resolved locally by a DNS server—meaning there is no matching record found either in its zone configuration information or local

cache—the query process will move forward based on the DNS server configuration. By default, recursion is configured on Windows 2008 DNS Server to resolve the query. Recursion refers to a process when a DNS server sends out queries to other DNS servers on behalf of a client. This, for the purpose of the query, turns the original DNS server into a DNS client.

If the default configuration is changed and recursion is disabled on a DNS server, iterative queries are performed by a DNS client. Iteration refers to a process when a DNS server will not forward the query to other DNS servers and instead responds to the client citing other DNS servers to which it should go. The client then will make multiple repeated queries to different DNS servers for resolution.

The recursive and iterative query process is illustrated in Figure 1.3.

Figure 1.3 The Iterative and Recursive Query Process



The following is the description of what events take place when a DNS client computer begins the query process:

1. The client sends out a query to NameServer1 seeking information on sales.nsoftad.com.

2. NameServer1 checks its local cache and zones database but can not find the matching record. It then contacts a root server, which is authoritative for the Internet, with the query for sales.nsoftad.com.
3. The Internet root server does not have the information and so responds with a referral to the server authoritative for .com domain.
4. Namerserver1 continues and sends out another query to .com Name server seeking information on sales.nsoftad.com.
5. The .com name server does not have the information on sales.nsoftad.com and so it responds with a referral to the server authoritative for nsoftad.com domain.
6. Namerserver1 continues and sends out another query to the nsoftad.com name server seeking information on sales.nsoftad.com.
7. The server authoritative for the nsoftad.com domain does have information on sales.nsoftad.com and responds with the IP address.
8. NameServer1 responds to the client query with the IP address for sales.nsoftad.com.

Query Response Types

Various types of answers can be sent to a client in response to a query. Most common responses are described in the following:

- **Authoritative Answer** This is a positive response to a DNS query in which the DNS server not only responds with the requested host record but also sets an authoritative bit in the DNS reply. This authoritative bit is an indication that this response is received directly by the authoritative server for the domain.
- **Positive answer** This is a response in which the answer received from the DNS server contains the requested information on the host address record.
- **Referral answer** This is a response in which the client does not actually get the requested information, but instead gets information on other DNS servers. These records provide a reference to other DNS servers that might be able to resolve the query. The DNS client computer can then send out queries to those DNS servers for name resolution by using iteration. This behavior occurs when recursion is not enabled on a DNS server. For example, you try to reach microsoft.com and the DNS client sends a query to the DNS server. DNS, however, does not have the record for

microsoft.com and so responds to the client with information on the .com DNS server, which may be helpful for resolution. If the DNS client is able to perform iterations, it then sends the query to the .com server for resolution.

- **Negative answer** This is a response by a DNS server when it encounters one of the two possible results while the DNS server is attempting to proceed and resolve the query recursively. It responds back to the client fully and authoritatively.
 - An authoritative DNS server reported that no such name exists in the DNS namespace that is requested in the query.
 - An authoritative DNS server reported that the host name exists, but that no record exists for the specified type requested in the query.

DNS Resource Records

Before we go further into DNS, let's review DNS resource records. Domain information is stored in *resource records*. An authoritative DNS server for a domain will contain all the resource records that are part of the domain for which it is authoritative. Ensuring the proper and accurate maintenance of these resource records is the responsibility of an administrator. DNS servers also store resource records in their cache when they resolve a query for a DNS client, which basically means DNS servers can store the host records from any part of the domain tree in its cache.

Many types of resource records are defined and supported by DNS servers. However, only certain types of records are used within Windows 2008 networks. These are described in Table 1.3.

Table 1.3 Resource Records Commonly Used in Windows 2008 Networks

| Record Type | Common Name | Description |
|-------------|--------------|--|
| A | Host address | Contains the name of a host and its Internet Protocol version 4 (IPv4) address. A computer with multiple network interfaces or IP addresses should have multiple host address records. |

Continued

Table 1.3 Continued. Resource Records Commonly Used in Windows 2008 Networks

| Record Type | Common Name | Description |
|--------------|-------------------|--|
| AAAA address | IPv6 host address | Contains the name of a host and its Internet Protocol version 6 (IPv6) address. A computer with multiple network interfaces or IP addresses should have multiple host address records. |
| CNAME | Canonical name | This creates an alias for a host name that allows a host to be known by multiple names in DNS. This is most commonly used when a host is providing a common service, such as World Wide Web (WWW) or File Transfer Protocol (FTP) and authors prefer to refer to it by a friendly name. For example, an administrator might want www.nsoftad.com to be an alias for the host srv1web.nsoftad.com . |
| MX | Mail exchanger | This indicates a mail exchange server for the domain. It allows mail to be delivered to the appropriate mail servers in the domain. For example, if an MX record is set for the domain nsoftad.com, all mail sent to <i>username@nsoftad.com</i> will be directed to the server specified in the MX record. |
| NS | Name server | This record provides a list of authoritative servers for a domain, which allows DNS lookups within various zones. All primary and secondary name servers in a domain should be defined through this record. |
| PTR | Pointer | This is used to enable reverse lookups by creating a pointer that maps an IP address to a host name. |

Continued

Table 1.3 Continued. Resource Records Commonly Used in Windows 2008 Networks

| Record Type | Common Name | Description |
|-------------|--------------------|---|
| SOA | Start of authority | This shows the authoritative name server for a particular zone. The best source of DNS information for a zone is its authoritative server. Each zone must have an SOA record. This record is created automatically when you create or add a zone. The information about how resource records in the zone should be used and cached is also included in the SOA. This includes refresh, retry, and expiration intervals and also the maximum time for which a record is considered valid. |
| SRV | Service location | This record enables the lookups to find a server providing a specific service. SRV records are used in Active Directory to locate domain controllers, global catalog servers, Lightweight Directory Access Protocol (LDAP) servers, and Kerberos servers. These SRV records are automatically created. For example, Active Directory creates an SRV record when you add a domain controller as a global catalog server. SRV records can also be added by LDAP servers to indicate they are available to handle LDAP requests in a particular zone. SRV records are created in the forest root zone. |

DNS Zones

Zone is a portion of namespace for which an authoritative server has full information and control. Zones are established to maintain boundaries within which a name server can resolve requests and replicate its zone information to other DNS servers. Resource records of one or more related DNS domains are stored in zones.

Windows 2008 supports four types of zones:

- **Standard Primary** There is a single master copy maintained of a zone. This copy is writable and kept as a text file. Any changes to the information of the zone are done in the primary zone. The primary zone information can be replicated to secondary zones.
- **Standard Secondary** This is a read-only copy of a zone stored as a text file in a DNS server. Since it is a read-only copy, updates to the zone information cannot be made. However, changes can be replicated from the primary zone to the secondary zone via zone transfers. The purpose of secondary zones is to provide redundancy and load balancing.
- **Active Directory Integrated** In Active Directory-integrated zones, the zone information is stored in Active Directory and this zone type uses Active Directory to perform zone transfers. This proprietary zone type is only possible with Active Directory deployed on the network. Active Directory-integrated zones were first introduced in Windows 2000. In Windows 2003 and Windows 2008, a feature is available to selectively replicate DNS information.

NOTE

Active Directory-integrated zones can only have domain controllers as a primary DNS server. Dynamic updates are required for Active Directory-integrated zones and only domain controllers have this capability. Due to security reasons, Active Directory allows the updates to domain controllers, but restricts the same from domain members.

- **Stub** A stub zone contains partial information on a zone—for instance, information only for the authoritative name servers of that zone. It has no information on other hosts that might be part of the zone. Using stub zones, queries can be directly forwarded to the authoritative name servers.

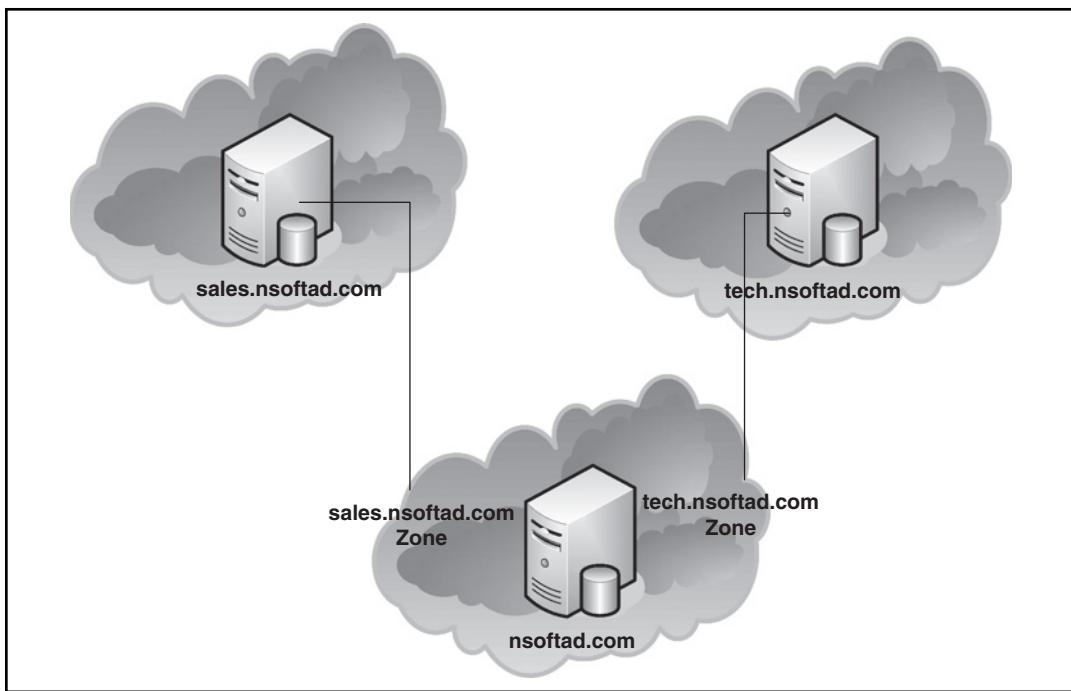
- **GlobalNames** This is a new feature in Windows Server 2008. The scope of this zone is the entire forest. The zone holds single-label names, which are very similar to what WINS hold in its database. However, this zone is meant to hold only a few host names and is not intended to hold records for all the machines in the zone. We will discuss this zone type in greater detail later in the chapter.

Non Active Directory–Integrated Zones

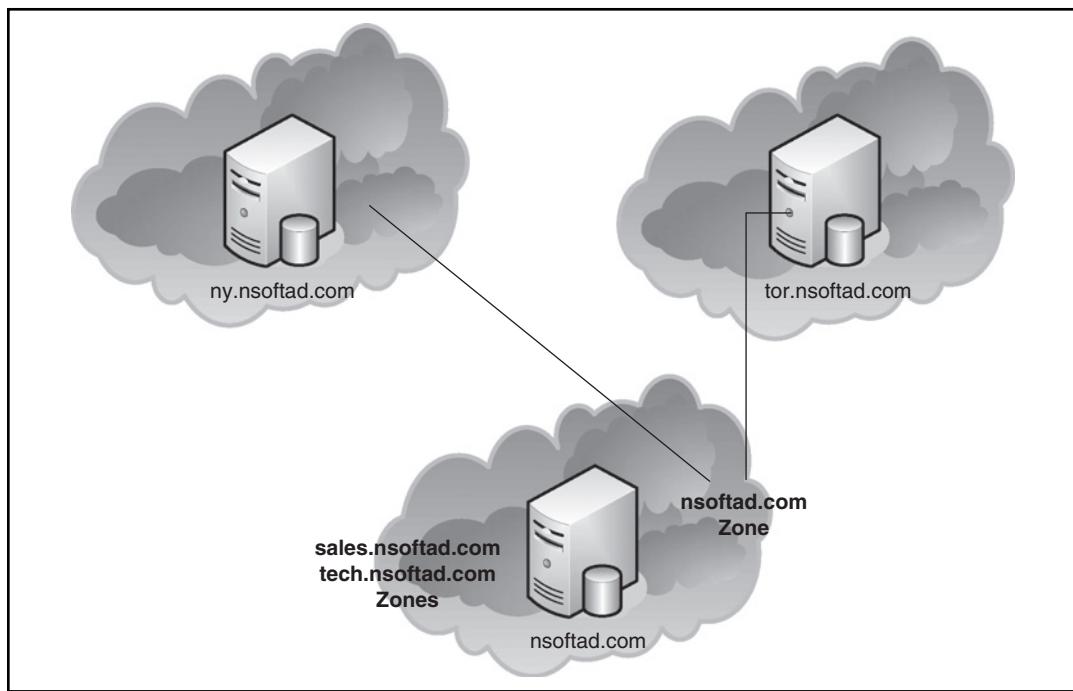
Standard zones are not integrated with Active Directory. In these zones, the primary zone holds a master copy of the zone information. This master copy is held by a single server known as the primary DNS server. The primary zone is indicated by the primary DNS server's SOA record for a particular domain. There can be other servers storing the copy of the zone and these servers are known as secondary DNS servers. These zones are called secondary zones and hold read-only copies. As such, no updates can be made directly on the secondary zone host records. The purpose of secondary zones is to maintain redundancy and improve performance.

The primary DNS zone information replicates from primary DNS servers to secondary zones in secondary DNS servers at preconfigured intervals. This process of replication is called zone transfer. In setting up a new secondary DNS server, initially the whole copy of the primary zone is transferred to the secondary zone. However, subsequent transfers are incremental since changes occur in the primary zone. This significantly reduces the amount of traffic required to do zone transfers from primary servers to the secondary servers since only the changes are replicated.

DNS zones can be implemented in many ways. You can implement your DNS zones so they mimic your domain structure. Figure 1.4 shows an example of how a company's domain structure can be used for zones and zone transfers. Separate zones handle name services for nsoftad.com, sales.nsoftad.com, and tech.nsoftad.com domains. In this example, users in sales.nsoftad.com and tech.nsoftad.com routinely work with servers in the nsoftad.com zone. For this reason, sales.nsoftad.com and tech.nsoftad.com domains are configured as a secondary zone, and the copies of the primary zone nsoftad.com are transferred to those secondary zones.

Figure 1.4 Zone Transfers Mimicking the Domain Structure

DNS zones do not necessarily have to follow the domain structure. Zone structure is independent of the domain structure. Parent and child domains can either be part of same zone or they can be part of another zone. These zones can be either on the same DNS server or separate DNS servers. For example, in the diagram in Figure 1.5, the branch offices in New York and Toronto are separate child domains and are running their own zones. On the other hand, the DNS server at the corporate head office is also hosting another zone alongside the `nsoftad.com` zone. This other zone is handling `sales.nsoftad.com` and `tech.nsoftad.com`.

Figure 1.5 Zones Configured Separately from the Domain Structure

Zones Integrated with Active Directory

In Active Directory–integrated zones, DNS zone information is stored within Active Directory. This approach offers several advantages. Any primary, stub, or globalnames zone that is integrated with Active Directory uses Active Directory replication to perform zone transfers to other DNS Servers. All DNS servers using Active Directory–integrated zones keep master read-write copies of the zone. For this reason, Active Directory–integrated zones can only be configured on domain controllers. With Active Directory–integrated zones, you can more efficiently replicate traffic since Active Directory can compress data in site-to-site replications. Especially for slower WAN links, this can be very useful.

There have been significant changes to Active Directory zones since their first implementation in Windows Server 2000. In Windows 2000, Active Directory stores the DNS information in the same context as other information in Active Directory. What this means is that all DNS zone information gets replicated to all domain controllers within the organization, regardless of whether those domain controllers are DNS servers or not. This can generate lots of unnecessary traffic, especially in a large environment with many domain controllers and only a few DNS servers.

In Windows Server 2003 and Windows Server 2008, the Active Directory default application partition is used. This to ensure that only those domain controllers that are also configured as DNS servers will get DNS information in replication. Separate application partitions within Active Directory are created for all the domains configured in the organization. These partitions store all the DNS records for their perspective domains. Because the context of the application partitions is outside that of other Active Directory information, DNS information is not replicated with other Active Directory information. There is also a separate application partition that contains DNS information and replicates it to all DNS servers in the forest. Utilizing these application partitions, you can configure the scope of the DNS server replications to the entire forest of DNS servers, domain DNS servers, or all the domain controllers.

NOTE

Windows Server 2008 introduces a new type of domain controller, the read-only domain controller (RODC). An RODC provides a read-only copy of a domain controller that cannot be directly configured or changed. This makes RODC less vulnerable to attack. You can install an RODC in locations where physical security for the domain controller is a concern. To support RODCs, a DNS server running Windows Server 2008 supports a new type of zone, the primary read-only zone (sometimes referred to as a branch office zone). When a server becomes a read-only domain controller, it replicates a full read-only copy of all the application directory partitions that DNS uses, including the domain partition, ForestDNSZones and DomainDNSZones. This ensures that the DNS server running on the RODC has a full read-only copy of any DNS zones stored on a centrally located domain controller in those directory partitions. The administrator of an RODC can view the contents of a primary read-only zone. However, the administrator can change the contents of the primary read-only zone only by changing the zone on the centrally located domain controller.

Among other benefits of Active Directory integration in Windows Server 2003 and Windows Server 2008, you can perform condition forwarding. In condition forwarding, you can define specific DNS servers to go to for a particular domain. It is especially useful in routing internal domain queries. Finally, secure dynamic updates can be enabled for clients via DHCP. This ensures that only those clients that created the original record can update the record.

Secondary Zones, Stub Zones, and Condition Forwarding

One of the biggest issues facing DNS is split-brain syndrome, where internal DNS servers blindly forward all the queries they can not resolve to external DNS servers. Secondary zones, stub zones, and conditional forwarding can be used to get around that problem. Instead of forwarding the requests blindly, internal DNS servers can be configured so they are aware of certain domains and thus forward the unresolved queries belonging to those domains to the DNS servers identified in conditional forwarding. This not only reduces the DNS traffic but also speeds up the name resolution process.

In stub zones, only the data needed to identify the authoritative name servers for a particular domain are transferred from the primary zone to the stub zone. These records include Start of Authority (SOA) and name server (NS) records. Stub zones can be implemented in two ways. They can be integrated with Active Directory, in which case, Active Directly replication takes care of the zone transfer. Or they can be a standard stub zone, wherein it uses standard zone transfer. In both cases, access to the domain specified in the stub zone is required, which can pose a security issue.

In conditional forwarding, however, no access is required to the specified domain. The name servers to which to conditionally forward the queries are manually defined in configuration of the conditional forwarding. For example, you define IP addresses of domain B name servers on DNS servers of domain A so they can forward any queries seeking domain B information. However, if the IP address of DNS servers in domain B changes, the changed IP address will not reflect on domain A DNS servers automatically. These would have to be manually updated.

The GlobalNames Zone

Today, many organizations deploy WINS in their networks. WINS is often used as a secondary name-resolution method alongside DNS. WINS is an older name resolution method used by Windows systems. WINS uses NetBIOS over TCP/IP (NetBT), which is approaching obsolescence. However, many organizations continue to use WINS because they appreciate having the static global records with single-label names that WINS provides.

So that organizations can move to an all-DNS environment (or to provide the benefits of global single-label names to all-DNS networks), the DNS Server service in Windows Server 2008 now supports a zone called GlobalNames to hold single-label names. Typically, the replication scope of this zone is the entire forest, which

ensures that the zone has the desired effect of providing unique single-label names across the entire forest. In addition, the GlobalNames zone can support single-label name resolution throughout an organization that contains multiple forests when you use Service Location (SRV) resource records to publish the location of the GlobalNames zone.

Unlike WINS, the GlobalNames zone is intended to provide single-label name resolution for a limited set of host names, typically corporate servers and Web sites that are centrally managed. The GlobalNames zone is not intended to be used for peer-to-peer name resolution, such as name resolution for workstations, and dynamic updates in the GlobalNames zone are not supported. Instead, the GlobalNames zone is most commonly used to hold CNAME resource records to map a single-label name to a fully qualified domain name (FQDN). In organizations currently using WINS, the GlobalNames zone can contain resource records for computer names already statically configured in WINS.

DNS Design Architecture

The following two primary DNS designs are currently used:

- Split-brain design
- Separate name design

Split-Brain Design: Same Internal and External Names

Split-brain design is implemented in many DNS architectures. In split-brain design, the organization uses the same domain name externally as it does internally. The name service is designed in a way that keeps the organization's external name resolution separate from its internal network and its internal name resolution traffic separate from its external network. Simply put, there are separate name servers for internal networks, and separate name servers for external networks. Otherwise, a big security risk may arise if your internal name servers are exposed externally to the public.

The major concern with this setup is that it totally isolates internal resources from public resources. From an internal user's perspective, it basically means that an internal user cannot access the external resources of the organization even though that information is available publicly to be accessed by everybody. So how to fix the problem? Luckily, the solution is simple. You can create records on an organization's authoritative DNS server for the internal network that specifies the IP address of

the organization's public resources. This solution allows internal users to access an organization's public resources but limits external users only to external resources—something which is good from a security perspective as well.

The following steps are needed to implement split-brain design:

- **Planning** Decide on what naming convention to use, how many servers are required for each domain, what type of zones to use, and so on.
- **DNS server installation and configuration** Install the DNS servers as defined in the planning and then configure the DNS service on those servers. If you are using Active Directory, you will find DNS server is already implemented on some servers, since DNS is required for Active Directory. In Active Directory–integrated zones, only those DNS servers that are also domain controllers can be holders of primary zones. If an Active Directory–integrated zone is configured on a DNS server that is not a domain controller, it can only be a secondary zone since it will not be able to update any records.
- **Create DNS records for public resources** On internal name servers, create records for all the publicly available Internet resources to allow internal users access to those resources. Typically, such services include, mail servers, www, and ftp servers.
- **Define forwarding to ISP's DNS servers** Your ISP provides you with the host names and IP addresses of its DNS servers to which you can forward your Internet name resolution queries. Your organization's internal DNS servers would need to be configured to forward all external queries to those ISP's DNS servers for all the queries they cannot resolve. You may also want to configure conditional forwarding of secondary zones to stub zones for the domains you would like to have direct access to, if required.
- **Configure internal network to use internal DNS servers** Configure all your internal systems to use your organization's internal name servers. All your workstations, servers, and any other equipment requiring name resolution should point to your internal name servers for all their DNS queries. If you have more than one DNS server in your organization, you may want to spread the priority list accordingly to spread the load among the servers.
- **Configure ISP's DNS server for internal resources** You may need to have your ISP's DNS server for some of your internal resources so those internal resources of your organization can be reached by the public.

One common example of this is having MX records point to mail servers in your organization. You would need to provide the host name and external IP address of the resource to your ISP for them to be configured.

Separate Name Design: Different External and Internal Names

In this approach to DNS design, a domain name used for your internal network is different than the domain name of your external or public network. This makes the organization's internal network separate from the external network. The advantage of this is that internal users can access the organization's external resources without issue since these are on separate domains. No additional configuration is required. Also, it removes the confusion of whether these resources are internally or externally within the organization. For example, a company such as Microsoft has the public DNS name of `microsoft.com`; however, it could use `microsoft.local` for its internal network.

The following steps are needed to implement a separate name design:

- **Planning** Decide on what naming convention to use, how many servers are required for each domain, what type of zones to use, and so on.
- **DNS server installation and configuration** Install the DNS Servers as defined in the planning and configure DNS services on those servers. If you are using Active Directory, you will find DNS server is already implemented on some servers since DNS is required for Active Directory. In Active Directory-integrated zones, only those DNS servers that are also domain controllers can be holders of primary zones. If an Active Directory-integrated zone is configured on a DNS server that is not a domain controller, it can only be a secondary zone since it will not be able to update any records.
- **Define forwarding to an ISP's DNS servers** Your ISP provides you with the host names and IP addresses of its DNS servers to which you can forward your Internet name resolution queries. Your organization's internal DNS servers would need to be configured to forward all external queries to those ISP's DNS servers for all the queries they cannot resolve. You may also want to configure the conditional forwarding; secondary zones are stub zones for the domains you would like to have the direct access to, if required.
- **Configure the internal network to use internal DNS servers** Configure all your internal systems to use your organization's internal

name servers. All your workstations, servers, and any other equipment requiring name resolution should point to your internal name servers for all their DNS queries. If you have more than one DNS server in your organization, you may want to distribute the priority list accordingly so as to spread the load among the servers.

- **Configure the ISP's DNS server for internal resources** You may need to have your ISP's DNS server accessible for some of your internal resources so certain internal resources of your organization can be reached by the public. One common example of this is to have MX records pointing to the mail servers of your organization. In this case, you would need to provide the host name and external IP address of the resource to your ISP for them to configure.

DNS Server Implementation

All Windows computers come with DNS service installed by default. However, DNS Server service is not installed by default and must be added. Once you have installed the DNS Server service, it will appear under Administrative Tools. There are various ways to install a DNS server. One is to have the DNS server installed along with Active Directory. A DNS server is required for Active Directory, and there are certain advantages to installing your DNS server when installing Active Directory Services, thus making Windows 2008 server a domain controller. In doing so, your forest and domain zones will be automatically created and configured with appropriate SRV records. The other way is to install DNS Server by adding a role in the Server Manager console. This option can be used for both domain controllers and member servers.

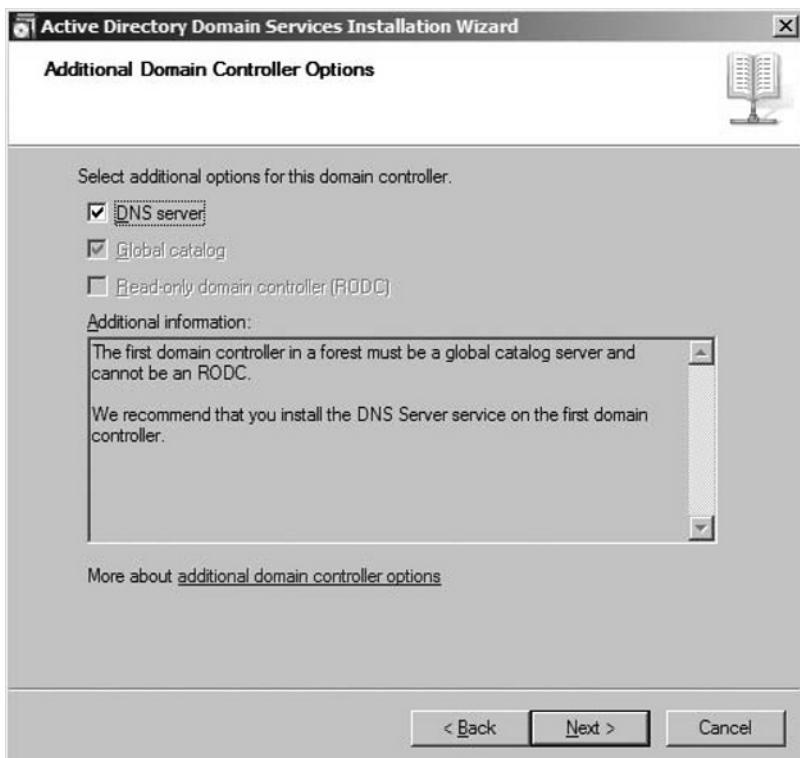
EXERCISE 1.1

INSTALLING WINDOWS 2008 DNS SERVER WITH ACTIVE DIRECTORY

1. Log on to a Windows 2008 Server with administrative privilege. This has to be a standalone server, not a domain controller. Ensure the server has a static IP address defined.
2. Click **Start | Run** and type **dcpromo**, then click **OK**. The system will check whether Active Directory has been previously installed on the machine and will continue to install Active Directory Services.

3. The Active Directory Wizard will appear. Click **Next**.
4. Click **Next** on the **Operating System Compatibility** page.
5. In the **Choose a Deployment Configuration** area, select **Create a new domain in a new forest**.
6. Below it, type the FQDN of the new forest root domain, enter the domain name you want to use, and then click **Next**.
7. Enter the domain NetBIOS name and then click **Next**.
8. For the Forest Functional Level, select **Windows Server 2008**.
(Please note that if you select a Forest Functional Level other than Windows Server 2008, you will also be prompted to select the Domain Functional Level.)
9. Additional Domain Controller options will appear. The DNS Server option checkbox will be selected. If it is not, mark the checkbox beside **DNS server** and click **Next** (see Figure 1.6). You will get a warning box if a static IP address is not defined.

Figure 1.6 A DNS Server Option When Installing a Domain Controller



10. If the delegation for DNS server cannot be created, the wizard will display a message indicating that the delegation can be created manually (see Figure 1.7). Click **Yes** to continue.

Figure 1.7 The Delegation Cannot be Created Message



11. On Location for Database, Log Files, and SYSVOL, leave the options as default and click **Next**.
12. Enter the Directory Services Restore Mode Administrator password and click **Next**.
13. Review the summary page and click **Next**.
14. DNS installation will begin, followed by the Group Policy Management Console, and creating the appropriate Active Directory Configurations.
15. On completion, click **Finish**.
16. You will be prompted to restart the server. Select **Restart Now**.
17. Once the server is booted, click **Start | Administrative Tools | DNS** to verify that the DNS server is installed successfully. You can configure the DNS server through this console as well.

EXERCISE 1.2

INSTALLING WINDOWS 2008 DNS SERVER VIA SERVER MANAGER

1. Log on to a Windows 2008 Server with administrative privilege. This can be either a standalone server or a domain controller. For the purpose of the next few exercises, however, choose a domain controller. Ensure the server has a static IP address defined.
 2. Click **Start | Administrative Tools | Server Manager**.
 3. In the left pane, right-click **Roles** and select **Add Roles**. This will bring up the Add Roles Wizard.
 4. At the Before You Begin message, click **Next**.
 5. Under the option, select one or more roles to install on this server, choose **DNS Server**.
 6. Click **Next**.
 7. On the **Introduction to DNS Server Information** page, click **Next**.
 8. On the **Confirmation** page, click **Install**. This will begin the DNS Server installation.
 9. Review the installation results and click **Close**.
 10. This will bring you back to the Server Manager console. In the right pane, under Roles Summary, you should see the DNS Server role installed.
 11. You can click **Start | Administrative Tools | DNS** to verify whether the DNS server was installed successfully. You can configure the DNS server through this console as well.
-

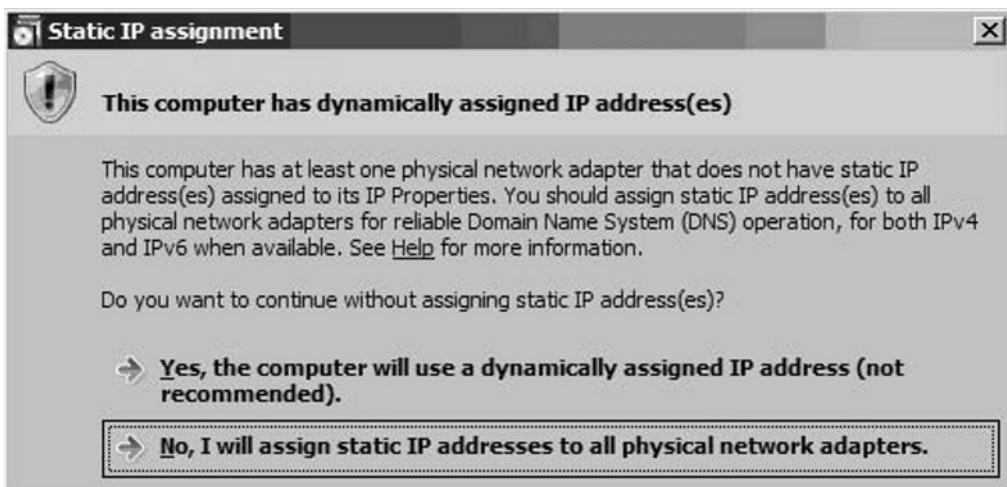
Head of the Class...

Use Static IP Addresses on DNS Servers

You should make it a practice to use static IP addresses on network critical services. Your domain naming servers should have static IP addresses. If you have clients configured to get DNS IP info from Dynamic Host Configuration Protocol (DHCP) or if they are hard-coded with DNS IP info, it is not a good idea to use dynamic IP addresses on DNS servers, where IP address of the DNS server could change over time. If you do not use the static IP address, you will get the error message shown in Figure 1.8.

Therefore, you should be using static addresses on DNS servers whether you are using IPv4 or IPv6. Assign static addresses for both IPv4 and IPv6 if both are enabled.

Figure 1.8 A Static IP Address Assignment Message



DNS Dynamic Updates and Security

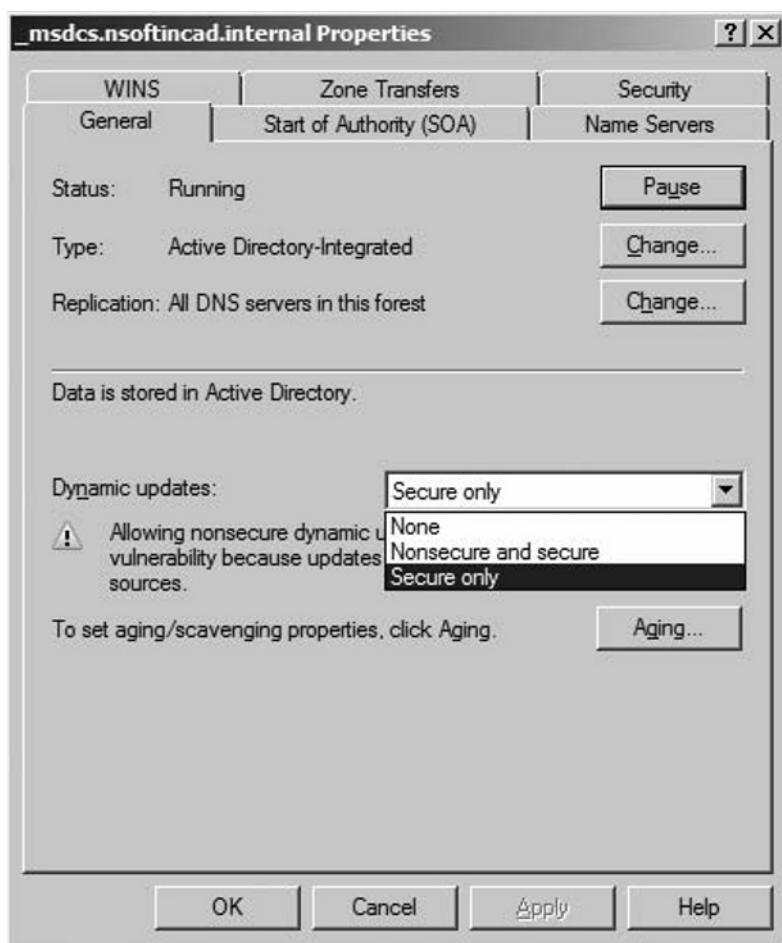
DNS dynamic updates are fully supported by Windows Server 2008. Dynamic updates are used in conjunction with DHCP server. This allows a DNS client to update its host record on the DNS server if its IP address changes and to allow PTR records of the client to be updated by the DHCP server. DHCP servers can be configured to update both the Host (A) record and the PTR record on behalf of a DHCP and DNS client. Windows Server 2008 also offers IPv6 support (AAAA records) for dynamic updates.

With dynamic updates enabled, DNS clients are expected to make their IP address change updates to the DNS server. Also, DHCP is expected to update the DNS server with the PTR record for the clients or update both the host records and PTR records, if configured that way. The two types of dynamic updates are:

- **Secure dynamic updates** In secure dynamic updates, a security mechanism is put in place that allows subsequent DNS updates only by the client that originally registered/created the record in the DNS server.
- **Nonsecure dynamic updates** In nonsecure dynamic updates, any machine can update the record. Thus, there is no way to ensure that only the client who originally created the record is updating the record.

When you create Active Directory–integrated zones, Secure dynamic updates are enabled by default. By doing so, only clients that are capable of registering themselves dynamically can update themselves. Please note that only clients from Windows 2000 and later can update their own records dynamically. Operating systems previous to Windows 2000 did not have the capability to do dynamic updates. DHCP server can be configured to dynamically update the host records for these clients on DNS server. You can change the setting from secure dynamic updates to both secure and nonsecure. You can also disable the dynamic updates all together.

In standard zones, by default, both secure and nonsecure dynamic updates are allowed. This way, not only can those clients who are capable of registering dynamic updates (Windows 2000 and later) perform the updates, but also older clients, who normally could not perform the dynamic updates. This setting seems to imply that security is involved; however, it simply means that the DNS server will accept both and not reject secure or nonsecure updates. Dynamic updates are registered from any client since DNS does not validate any updates. A security risk exists with this since client updates can be registered from untrusted sources. You can set this in Zone properties, as shown in the Figure 1.9.

Figure 1.9 Dynamic Update Settings in Zone Properties

Creating Zones and Host Records

We have already covered zones earlier in the chapter, so in the following exercise we will create a zone. Notice that several records are automatically created when creating a zone in Windows Server 2008.

- In Forward lookup zones, the SOA record, NS record, and the A record are automatically created. The SOA record contains information about the behavior of resource records in a zone, such as how they should be used or cached. An NS record contains the authoritative name server for the

configured zone. The A record is of the host address record for the DNS server on which you configured the zone.

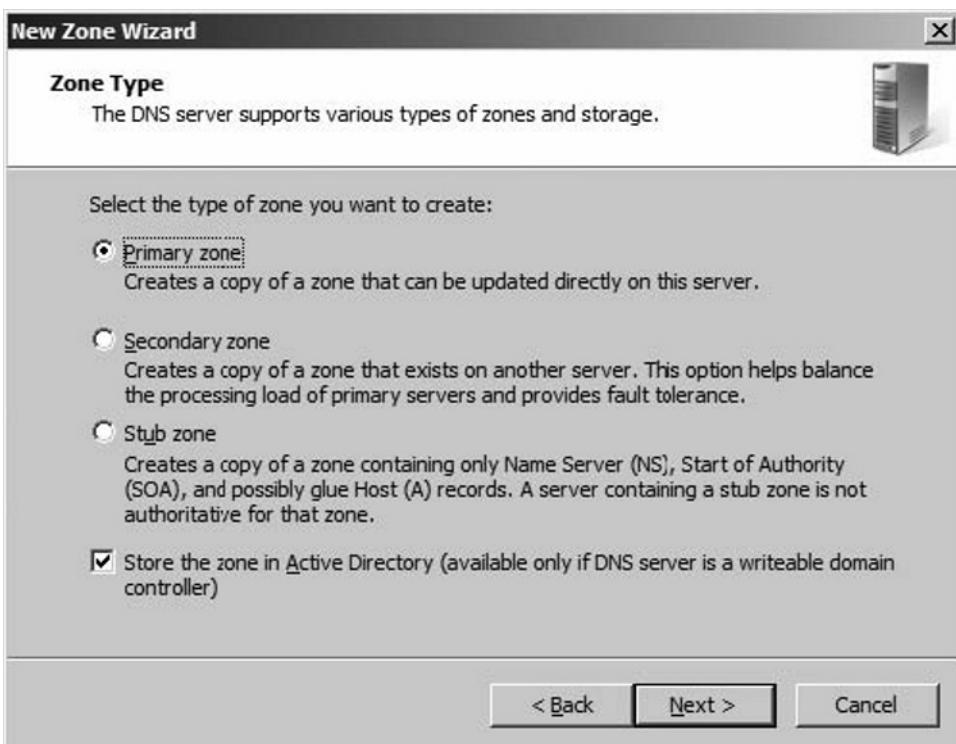
- In Reverse lookup zones, the SOA record, NS record, and PTR record are automatically created. The SOA record contains information on the behavior of resource records in a zone, such as how they should be used or cached. An NS record contains the authoritative name server for the zone configured, while the PTR record is the pointer record of the DNS server you configured the zone on to allow reverse lookups by the IP address.
- If the zone is Active Directory–integrated, SRV records for domain controllers, global catalog servers, and PDC Emulator are automatically created.
- If dynamic updates are allowed, A records are automatically created for the clients. If DHCP is configured for dynamic updates, PTR records of the clients are automatically updated as well.

EXERCISE 1.3

CREATING A ZONE

1. Log on as Administrator to a Windows 2008 Server with DNS Server service installed.
2. Click **Start | Administrative Tools | DNS**.
3. Right-click **Forward Lookup Zones** and select **New Zone**.
4. Click **Next** on the welcome screen of the wizard.
5. The **Zone Type** page appears. Select **Primary Zone** (see Figure 1.10).
6. Note the option at the bottom to store the zone in Active Directory. Select the checkbox. This will create the zone as Active Directory–integrated. Click **Next**.
7. In the Active Directory Replication scope, select **To all DNS servers in this domain** and then click **Next**.
8. Type the name of the zone **Testzone1** and click **Next**.
9. Choose dynamic update settings. Select **Allow only Dynamic updates** (recommended for Active Directory) and then click **Next**.
10. Review your settings and click **Finish**.

Figure 1.10 Choosing the Zone Type



NOTE

If you are creating a secondary zone, the option of Store The Zone In Active Directory will be grayed out since you will be creating a read-only copy of the master primary zone. No changes can be made to it and this zone is not replicated to other servers.

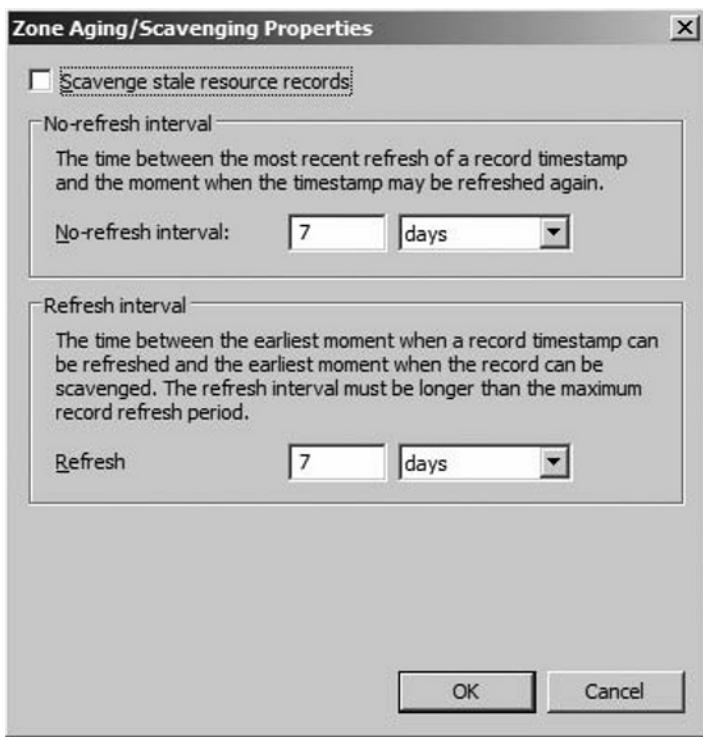
Setting Aging and Scavenging

Records in the DNS server are not cleaned by default. This seems to be fine for all the records you have manually created. However, for clients with dynamically assigned IP addresses, what this means is that old records that are no longer in use might still be in the DNS server database.

You can use the Aging and Scavenging feature on the DNS server to overcome this problem. This feature lets you set rules on how long the dynamically created record will be valid and if the re-registration of the dynamic record does not happen, to clear out the record. The Aging and Scavenging setting can be applied at these two levels:

- **Zone** Zone-level aging and scavenging policies apply to an individual zone on a DNS server. To set a zone-level rule:
 - a. Right-click a zone entry in the **Nodes** pane.
 - b. Click **Properties**.
 - c. On the **General** tab, click the **Aging** button.
- **Server** Server-level aging and scavenging policies apply to all zones on a DNS server. To set a zone level rule:
 - a. Right-click a server entry in the **Nodes** pane.
 - b. Click **Set Aging/Scavenging for all Zones**.
- Once you set the aging/scavenging rule and click OK, another message will display, informing you that these settings will be applied to new Active Directory-integrated zones created on the DNS server. If you want to apply these settings to existing zones, select the checkbox **Apply these settings to existing Active Directory integrated zones** and click **OK**.

In both of the preceding cases, the dialog box to set aging and scavenging rules is similar to that in Figure 1.11.

Figure 1.11 Aging and Scavenging Options

To enable aging/scavenging, select the checkbox **Scavenge stale resource records on top of the dialog box** and then click **OK** after you have set the rules. These rules are:

- **No-refresh interval** This sets a minimum time during which a dynamic DNS client cannot reregister or update its DNS record. The default is set to an interval of seven days. What it means is that if the DNS client tries to reregister its records in the DNS server during the seven days after the client creates the DNS record, the DNS server will simply ignore the request. The reason for this setting is that whenever a record reregisters, it must be replicated, since it is seen as a change in the database. This no-refresh interval setting does not affect the reregistration of clients whose IP address has changed. When the IP address is changed, the old record is removed and the new record is registered.
- **Refresh interval** This is the time between the earliest moment a record can be refreshed and the earliest moment it can be scavenged. It is the combined extent of the no-refresh interval and the refresh interval, before

which records cannot be deleted. The default setting for this rule is also seven days, the same as a no-refresh interval. This gives a total number of 14 days. It means records cannot be scavenged by the DNS server until they are older than 14 days.

NOTE

You can also initiate the scavenging of stale (old) records manually. To do this, right-click the server entry in the DNS console and select **Scavenge Stale Resource Records**. Click **Yes** when prompted to confirm.

You can also start scavenging at the command prompt by using the **dnscmd** command. Go to the command prompt and type **dnscmd Servername /startscavenging**, where Servername is the name or IP address of the DNS server you would like to perform scavenging on.

Configuring DNS Client Settings

The following needs to be performed (at minimum) to connect DNS clients in Windows Server 2008 networks:

- Set a host name or DNS name for each computer on the network.
For example, in FQDN computer1.nsoftincad.internal, the left-most label is the host name or the computer's DNS name.
- Set a primary DNS suffix for the computer. The full computer name is formed when the suffix is added to the host name. In the previous example, the primary DNS suffix was nsoftad.com.
- Set the DNS servers list for the client. Without this client, you would not know where to go to resolve DNS names. This list can include just the primary DNS server, or it may include additional alternate servers to go to if the primary DNS server is not available.

Depending on the need for client configuration, you may also have to perform some of the following settings:

- Set the DNS suffix search order or method to be used by the client when it performs a DNS query searching for short unqualified domain names.
- Set a connection-specific DNS for each network adapter on a DNS client. For example, if a DNS client named computer1 is multihomed or

connected to different networks, it can be seen on both networks—on one as computer1.network1.nsoftad.com and on the other as computer1.network2.nsoftad.com.

- Change the Dynamic DNS (DDNS) update behavior.

These tasks are described in more detail in the following section.

Setting Computer Names

The computer name or the host name is the leftmost label of a FQDN. For example, in FQDN computer1.nsoftincad.internal, computer1 is the host name. You can also view and modify this computer name by going to the system properties and then to the Computer Name tab.

NOTE

You can access the system properties by going to the Control Panel and double-clicking the System icon, or by right-clicking My Computer and choosing Properties.

The computer name you assign must be according to the Request For Comments (RFC) 1123, which outlines some restrictions on what characters you can use for host names. According to the RFC restrictions, you cannot use more than 63 characters, and the name can include any of the following characters:

- Uppercase letters, A through Z
- Lowercase letters, a through z
- Numbers, 0 through 9
- Hyphens (-)

NOTE

In general, DNS host names are not case-sensitive.

NetBIOS Names Accommodation

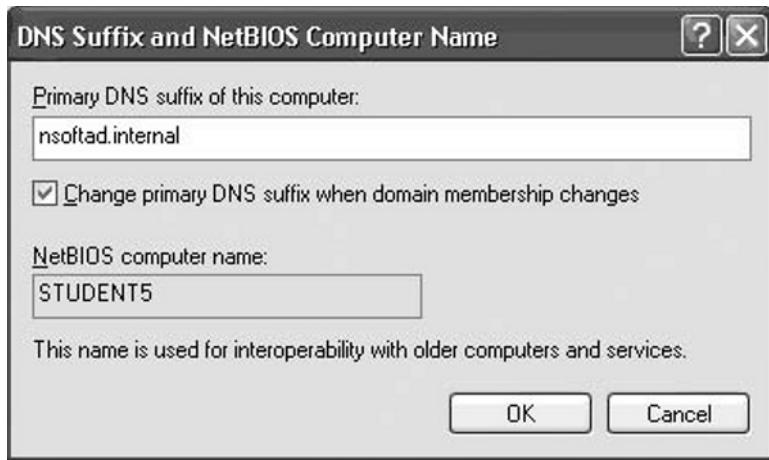
All Windows computers have a NetBIOS name in addition to their host name. You can assign different names and DNS host names than the NetBIOS name. However, this is not recommended since it can cause some name resolution issues. Even though DNS names can extend to 63 characters, NetBIOS names are limited to 15 characters in length. Keep that in mind when you are planning your naming strategy so as to limit your computer names to 15 characters.

Setting the Primary DNS Suffix

You can set the computer's primary DNS suffix in the DNS Suffix and NetBIOS Computer Name dialog boxes (see Figure 1.12). By default, this primary DNS suffix would have the same name as the name of the domain computer it belongs to. If the computer is not part of the domain, no primary DNS suffix will be defined here.

You can change the primary DNS suffix by going to the **Computer Name** tab in **System Properties** and clicking **Change**. Click **More** in the **Computer Name Change** dialog box.

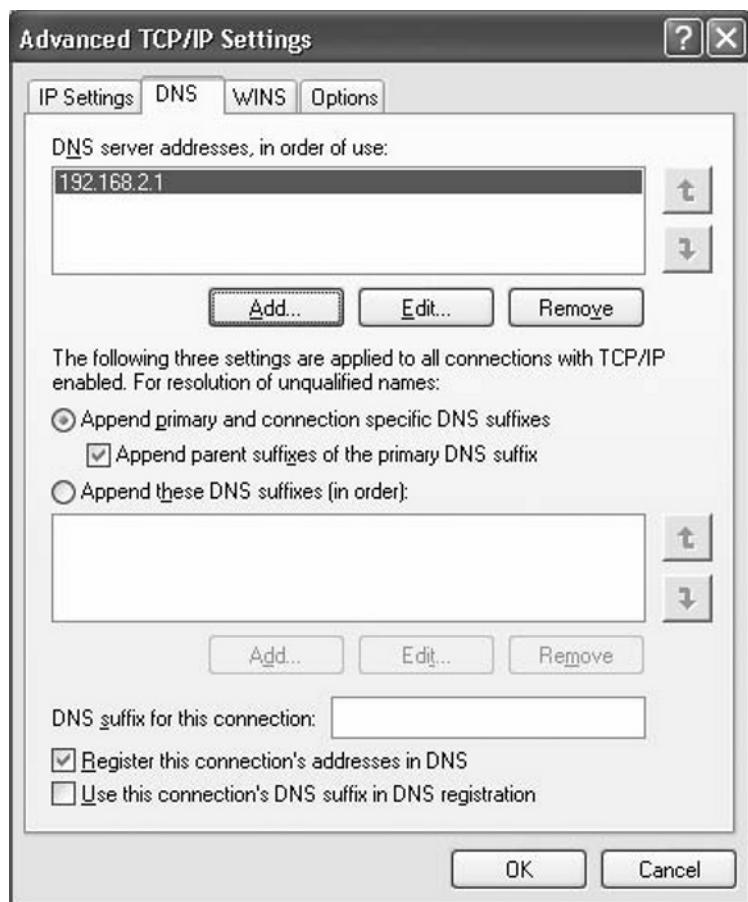
Figure 1.12 Specifying the Primary DNS Suffix



Setting Connection-Specific DNS Suffixes

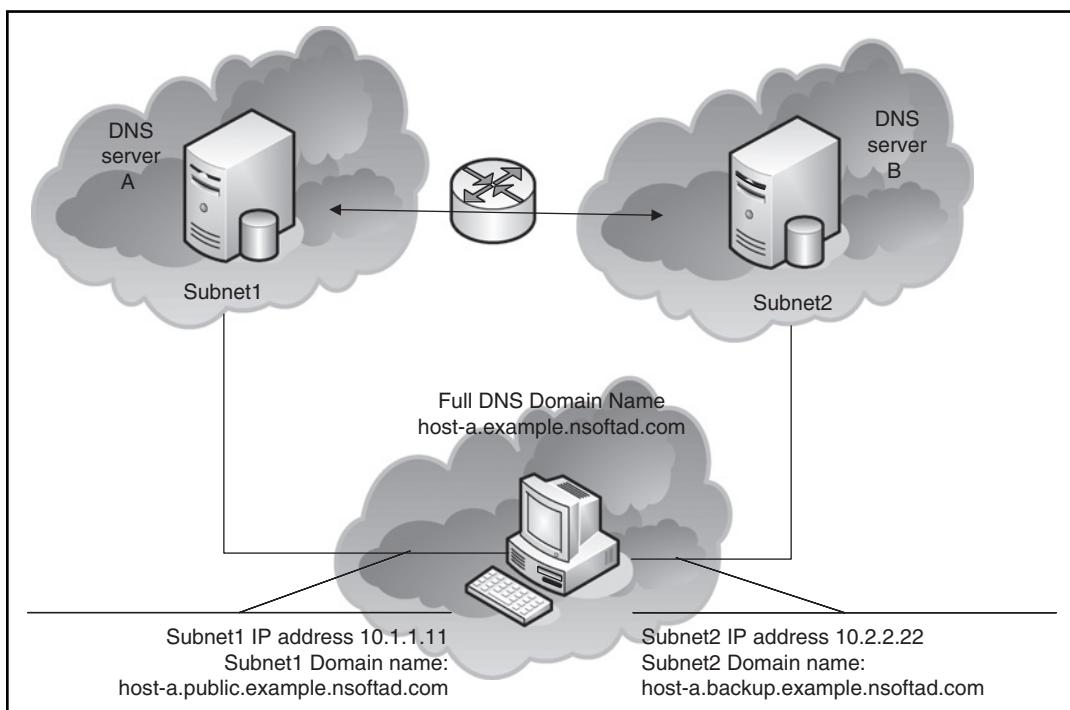
To access these settings, you must go to the **Advanced** tab in the TCP/IP properties of the particular network adapter you are working with. Then, click the **DNS** tab. A dialog box will appear, as shown in Figure 1.13.

Figure 1.13 The DNS Tab in the Advanced TCP/IP Properties Window



Here you can create a DNS suffix to be specifically used by this network interface. The suffix you define here is called a connection-specific DNS suffix. An FQDN is assigned to the particular adapter on the computer when you assign a connection-specific DNS suffix to a computer.

For example, a multihomed computer host—a can be named both, by its primary DNS suffix as well as by its connection-specific DNS suffix (see Figure 1.14).

Figure 1.14 Using Connection-Specific DNS Suffixes

In Figure 1.14, notice that host-a is attached to two separate networks—subnet 1 and subnet 2. Both of these networks are connected to each other, with a router in between. The host-a computer can be accessed by both of these networks using separate names. It can also be accessed by its own FQDN as well. When configured as shown here, a client running Windows 2000, Windows XP, Windows Server 2003, or Windows Server 2008 can register host (A) records in DNS with its three unique names and the IP addresses belonging to them, as shown in Table 1.4.

Table 1.4 The FQDN of a Multihomed Computer

| DNS Name | IP Addresses | Description |
|-----------------------------------|-------------------------|--|
| host-a.example.nsoftad.com | 10.1.1.11, 10.2.2.22 | This is the full computer name. The computer registers A and PTR resource records for all configured IP addresses under this name in the example.nsoftad.com zone. |
| host-a.public.example.nsoftad.com | 10.1.1.11 | This is the connection-specific DNS name for LAN connection 1, which registers A and PTR resource records for IP address 10.1.1.11 in the public.example.nsoftad.com zone. |
| host-a.backup.example.nsoftad.com | 10.2.2.22 | This is the connection-specific DNS name for LAN connection 2, which registers A and PTR resource records for IP address 10.2.2.22 in the backup.example.nsoftad.com zone. |

The DNS Resolver Cache

The DNS resolver cache is client-side caching of DNS query responses. It is also known as the DNS client cache. It is maintained by a DNS client and is totally separate from the DNS server cache. Whenever a client needs to resolve a DNS name, it checks in its cache first before sending out the query to a DNS server. If a record is found, the query is resolved locally and isn't sent out. If there is no record, the query is sent out and the response received is cached in the local DNS resolver cache to resolve any subsequent requests for the same DNS name.

The DNS resolver cache can be flushed by either running the `ipconfig /flushdns` command or restarting the DNS client service. This can be done either through the services console or by restarting the client computer.



EXAM TIP

Remember the following DNS-related commands for the exam:

- **Ipconfig /displaydns** Displays the contents of the DNS resolver cache on the client
- **Ipconfig /flushdns** Purges the contents of the DNS resolver cache on the client
- **Ipconfig /registerdns** Refreshes the DHCP lease of the client and re-registers the host name with the DNS server if the zone is configured to accept dynamic updates

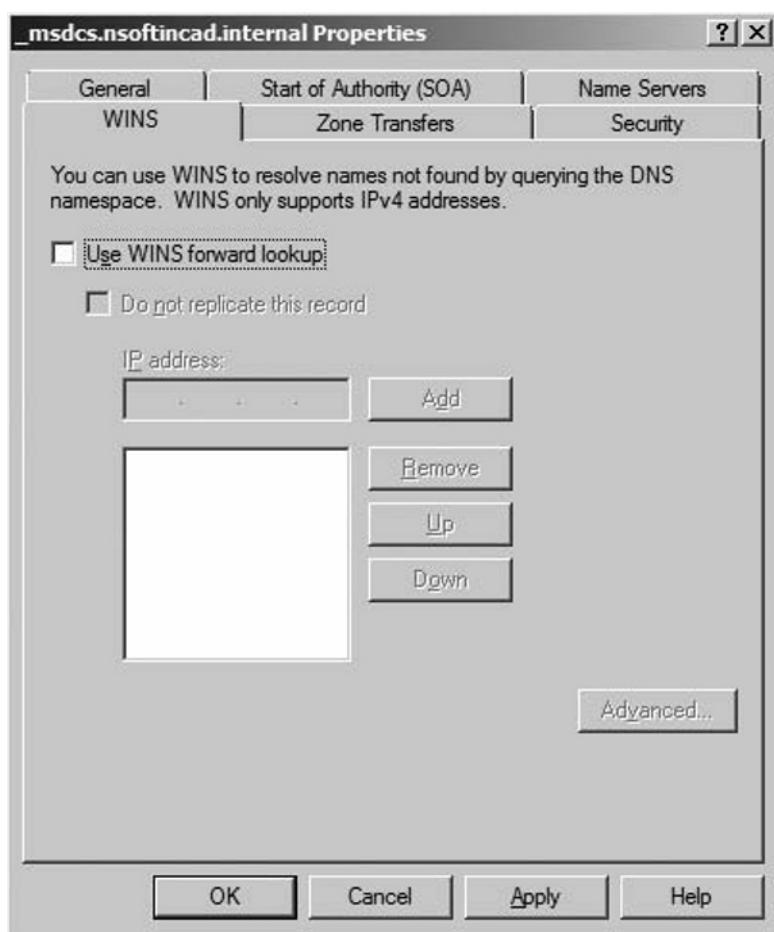
Also note that dynamic updates can be performed only on Windows operating systems Windows 2000 and later.

Nslookup

With the *nslookup* command, you can query a DNS server and view the information a particular DNS server holds for a host record. By using this command, you are querying a server in iterative mode, which means the DNS server will not go out to resolve the query and will only give the result from its own DNS database.

Integration with WINS

If your environment has heavy reliance on WINS or NetBIOS names, you can integrate your WINS server with the DNS server. By utilizing the WINS lookup feature in the Windows Server 2008 DNS server, you are enabling the DNS server to query the WINS server to see if the record exists. If the record exists, the DNS server will create a record in its own zone database. This is done at the zone level. You set this at the zone properties, as shown in Figure 1.15. This is helpful in reducing traffic and name resolution time when you already have the DNS server configured in the environment as the primary name resolution method.

Figure 1.15 WINS Integration in Zone Properties**EXAM TIP**

When a WINS lookup for a forward lookup zone is configured, a WINS resource record pointing to the WINS server you specify is created and added to the zone database. When you create a WINS-R lookup for a reverse lookup zone, the WINS-R record is added to the zone database, pointing to the WINS server you specify in the WINS tab.

The HOSTS File

The HOSTS file is a text file that provides DNS name mapping to IP addresses. This file is locally available on a computer. When a DNS name resolution is required, the DNS clients will look into the HOSTS file before sending out the query to a DNS server.

The path to this file is `%systemroot%\WINDOWS\system32\drivers\etc`. This file has no extension. The entries in the file are not dynamic and are manually updated. Typically, you will not configure this file with entries since this file is specific to the computer you are working on. Hence, the entries will only apply to the computer where this file is updated. Also, if the host record is changed, the changes are not reflective automatically. Thus the computer would have no information on updating the record and will keep mapping the IP address to a host name as it is in the HOSTS file.

The following is a sample HOSTS file:

```
# Copyright (c) 1993-1999 Microsoft Corp.  
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#      102.54.94.97    rhino.acme.com        # source server  
#      38.25.63.10     x.acme.com            # x client host  
127.0.0.1      localhost
```

Another name resolution service supported by Windows is WINS. WINS uses the NetBIOS protocol. All computers under WINS have NetBIOS names. WINS provides mapping for NetBIOS names to the associated IP addresses just as DNS provides mapping for host names to IP addresses.

NetBIOS works on broadcast and it was the primary naming system supported by Windows Systems prior to Windows 2000. It is still used in Windows networks to maintain backward compatibility with Windows 95, Windows 98, and Windows NT. The advantage of using NetBIOS is that it can work without any configuration.

NetBIOS names are limited to a maximum length of 15 characters. All NetBIOS names must be unique within a network. WINS maintains records for the computers with NetBIOS names within its network. Both forward lookup (where NetBIOS names are resolved to IP addresses) and reverse lookup (where IP addresses are resolved to NetBIOS names) are supported by WINS.

Because NetBIOS works on broadcast, every computer in the network listens in on what other computers are communicating. This adds unnecessary traffic on the network. Though this works well for small networks, as the network grows, it becomes inefficient. Also, NetBIOS is a nonroutable protocol, which means it does not go beyond the network segment.

To get around the routability problem, Microsoft developed NetBIOS over TCP/IP, also called NBT. NBT still sends out broadcasts but allows NetBIOS name resolution on TCP/IP networks. This still cluttered the network, so another solution was created, known as WINS.

WINS listens to NBT broadcasts and collects them in a central store. The store contains the NetBIOS computer names and their associated IP addresses. If Windows clients are configured to use WINS server, they contact WINS for any NetBIOS name resolution before sending out the broadcast. This solution reduces the network load.

Because NBT clients work on broadcast, you need to configure them to use WINS. Therefore, you need to be familiar with some of the terminologies. Node types are methods clients use to resolve NetBIOS names (see Table 1.5). Node types are configured in NBT settings on clients. The client node type can be changed via the Registry; however, it is better to use DHCP or leave the settings as their defaults.

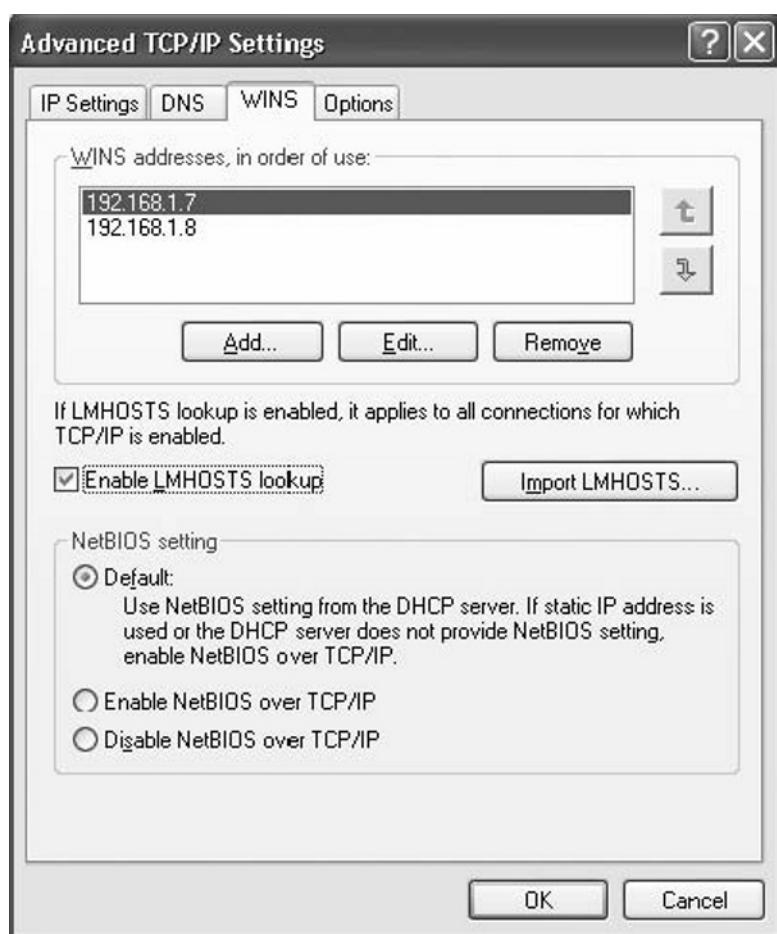
Table 1.5 NetBIOS Node Types

| Node Type | Description |
|-------------------------|--|
| b-node (broadcast) | Broadcasts NBT queries for name registration and resolution. This is the default for Windows 2000, XP, and Windows Server 2003 client machines not configured with WINS. Good for small networks. |
| p-node (peer-peer node) | Uses a NetBIOS name server (or a WINS server) to resolve NetBIOS names and does not use broadcasts. It is the best option if you want to eliminate broadcasts from your network. Sometimes a resource might not be seen as available if the WINS server is not updated properly. |
| m-node (mixed) | This is a combination of b-node and p-node, and is, in its default, similar to b-node. If it cannot resolve a name by broadcast, it tries to access WINS server for resolution. This still generates much broadcast traffic. |
| h-node (hybrid) | In its default, it is similar to p-node. If it cannot resolve a name, it reverts to b-node. This is the default for Windows 2000, XP, Windows 2003, and Windows Server 2008 client machines configured with WINS. |

Configuring Information for WINS Clients

All Windows computers have a WINS client, which is installed automatically by default. If you go to the TCP/IP advanced settings under TCP/IP properties, you can find WINS settings there on the WINS tab. These are located in the network connection properties of a client. The tab offers a group of options you can configure on your client to use in WINS for name resolution (see Figure 1.16).

Figure 1.16 The WINS Tab in the Advanced TCP/IP Settings Dialog Box



The various controls and options in Figure 1.16 are as follows:

- **Wins Address** This list and its related controls show you which WINS servers you have defined for this client. The list is empty by default. You can add WINS servers manually to it if you want to use WINS, or you can use DHCP to define WINS servers for the client. Similar to DNS, the WINS code will send WINS resolution requests to the servers on this list and in the priority order of their appearance. If the first server is not available or does not respond, the name resolution request goes to the second server in the list, and so on. You can add, remove, and change server addresses with the buttons shown below the list. You can also change the

ordering of the servers by selecting a server and using the up and down arrow buttons shown on the list's right side. Up to 12 WINS servers can be defined on the list.

- **LMHOSTS** This is the next group, which is shown immediately below the WINS address list group. Here, you can control whether or not the old-style *LMHOSTS files* should be used as a source for address resolution information. The LMHOSTS file is a simple text file that contains mappings for NetBIOS names and their IP addresses. This file can be referenced by computers to resolve names to IP addresses, or they can resort to traditional broadcasts or WINS methods. The Enable LMHOSTS Lookup checkbox controls whether or not Windows Server 2008 will use the computer name to IP mappings in the LMHOSTS file before running a query against a WINS server. When you check this box, LMHOSTS lookups are enabled not only for the connection whose properties you're editing, but for all connections that are using TCP/IP. The Import LMHOSTS button lets you load the contents of a file into the WINS name cache, which is useful if you want to load a set of name mappings without keeping a file on a local disk.
- **NetBIOS Setting** The final controls are the three radio buttons at the bottom of the dialog box. They control whether NetBIOS over TCP/IP is active at all. In the past, NetBEUI was the only transport that could carry NetBIOS traffic, but it wasn't routable and had poor performance on large networks. As you saw earlier, Windows Server 2003 includes support for NBT, even though we expect its use to diminish as networks move toward pure TCP/IP. Here's what each button does:
 - **Default: Use NetBIOS Setting From The DHCP Server button.** This forces the client to use the DHCP server's setting instead of manual settings for WINS or the LMHOSTS file. If this button is *not* selected, whatever setting is in place will override the DHCP server's setting.
 - **The Enable NetBIOS Over TCP/IP button.** If this is selected, it will override a DHCP setting. It allows this client to communicate via NetBIOS traffic with servers using TCP/IP as a transport.
 - **The Disable NetBIOS Over TCP/IP button.** If this is selected, it will turn off NBT for this client. This is useful when you want to totally free your network of all NetBIOS traffic, even when it is encapsulated and when WINS or NetBIOS are not used on your network at all.

EXERCISE 1.4

CONFIGURE A WINDOWS SERVER 2008 MACHINE AS A WINS CLIENT

1. Select **Start | Control Panel | Network and Sharing Center**.
2. On the right side under Tasks, click **Manage Network Connections**. This will bring you to the Network Connections dialog box.
3. Right-click the **Local Area Connection (LAN)** icon and choose **Properties**. If you have more than one LAN adapter, choose the connection you want to configure.
4. The **Local Area Connection Properties** dialog box appears. Select **Internet Protocol Version 4(TCP/IPv4)** from the **This Connection Uses The Following Items** list.
5. Click the **Properties** button. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box appears.
6. Click the **Advanced** button. The **Advanced TCP/IP Settings** dialog box appears.
7. Click the **WINS** tab.
8. Click the **Add** button. When the **TCP/IP WINS Server** dialog box appears, enter the IP address for your WINS server and click the **Add** button. The first WINS server on the list is a primary WINS server and should be the server physically closest to the client machine. You can enter additional WINS server addresses and rearrange the server priorities as necessary if you like.
9. Click **OK** to close the Advanced TCP/IP Settings dialog box.
10. Click **OK** to close the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
11. Click **OK** to close the Local Area Connection Properties dialog box.

WINS Name Registration and Cache

WINS server automatically maintains a mapping of its computer-name-to-IP-address in its database. When a computer or resource becomes available, it sends a broadcast and registers itself with the WINS server, telling the server the name and IP address it is using. As long as no other computer or resource on the network is

using the same name, the WINS server accepts the request and updates its database with the registration of the computer or resource.

This Name registration is not a permanent record. Each registered name in the WINS database has a lease period associated with it, which is known as its Time to Live (TTL). A WINS client must reregister its name with the WINS server before the lease expires. The lease reregistration attempt by the client is initiated when the client is restarted or when 50 percent of the lease period has elapsed. If a WINS client fails to reregister its name with WINS server, the lease expires and is marked for deletion from the WINS database. When shutting down normally, a WINS client will also send a message to the WINS server telling it that it is no longer available and requesting release of the registration. At this point, WINS server marks the record for deletion from its database. Those records that are marked for deletion are said to be tombstoned.

Similar to DNS clients, the cache of looked-up NetBIOS names is maintained by WINS clients. However, the WINS cache is designed to hold recently looked-up names only. By default, names are cached for a duration of ten minutes. This cache is also limited to 16 names. Entries in the NetBIOS cache can be viewed by typing *nbstat -c* at the command prompt.

Remember the following NetBIOS-related commands:

- **nbtstat -c** Lists the names in the local NetBIOS name cache
- **nbtstat -R** Purges the local NetBIOS name cache

Setting Up a WINS Server

Typically, in an environment with WINS, at least two servers are configured as WINS servers. With multiple WINS servers in an environment, the replication of databases between the WINS servers can be configured by the administrator. By ensuring that a WINS server's database records are replicated to its partners, such replication allows for redundancy and fault tolerance. All the WINS replication partners can then handle all client requests such as name resolution, name and IP registration, and renewals.

To enable a computer running a Windows 2008 server as a WINS server, you need to install WINS service. This service does not require many resources and adds very little overhead. Hence, it does not require a dedicated server. It can be installed on any server such as a DHCP server, DNS server, or even a domain controller; however, it is not recommended it be installed on a domain controller. One requirement though is that the server has a static IP address assigned.

EXERCISE 1.5

INSTALLING WINS SERVER

In Windows 2008, WINS server is referred to as a Server feature, and is installed through Server Manager. There are two ways to get to Server Manager.

1. Through the Control Panel: Choose **Control Panel | Programs and Features**.
2. In Programs and Features, on the right side you will see Tasks. Under Tasks, double-click **Turn Windows Features on or off**.

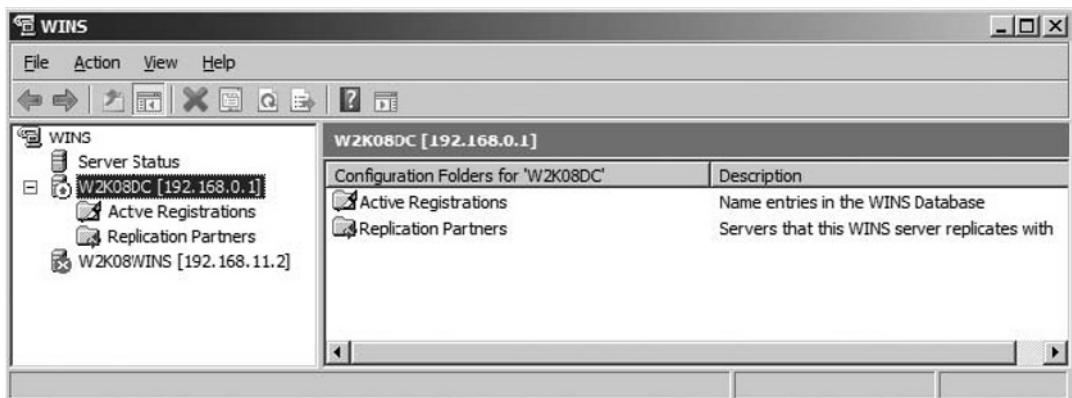
Alternatively, you can go to **Administrative Tools** and click **Server Manager**.

1. Once in Server Manager, on the left pane right-click **Features** and select **Add Features**. This brings you to the Add Features Wizard.
2. In the **Add Features Wizard**, select **WINS** server from the list. Once the WINS server selection box is checked, click **Next**.
3. Confirm your selection and click **Install**.
4. Close the window upon successful installation.

Configuring WINS Server

To configure WINS, go to **Start | Administrative Tools | WINS**. This will open up the WINS Management Console as shown in Figure 1.17.

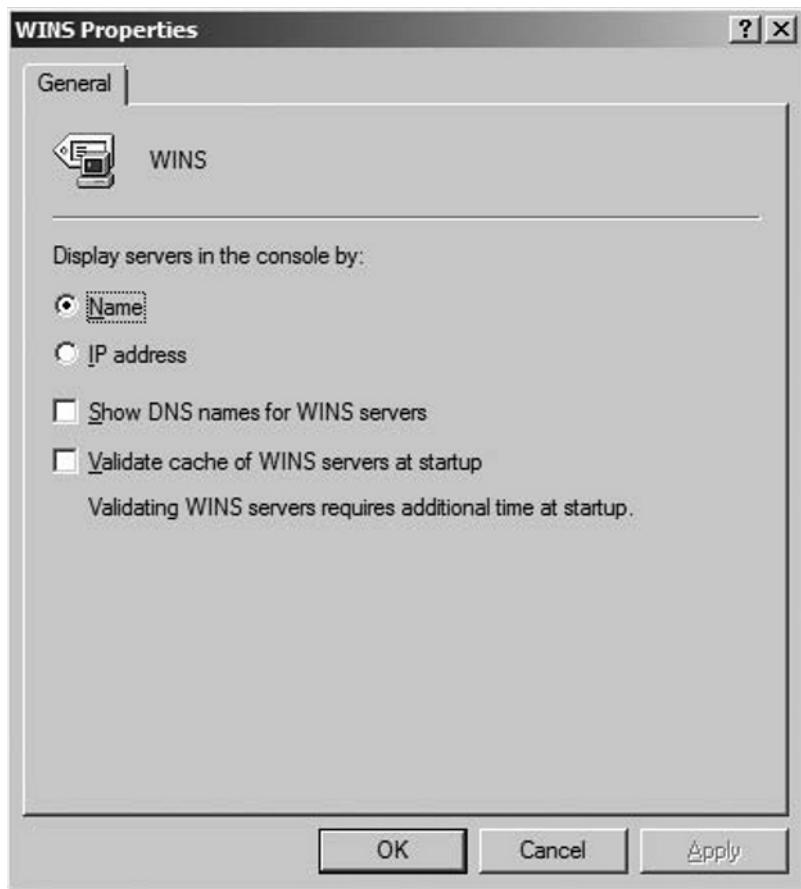
Figure 1.17 The WINS Management Console



On the left Nodes pane, a number of items, called nodes, are listed. These nodes are described next:

- **WINS** The first node listed on top of the hierarchy is WINS. If you click WINS, you will see the list of WINS servers defined by the administrator. Here you can also see which servers are connected and which ones are not. Right-click WINS and go to properties. The window shown in Figure 1.18 will appear.

Figure 1.18 WINS Server Properties



The options shown in Figure 1.18 are self-explanatory. With the exception of the last option of validating the cache of WINS servers, the other three options deal with how you want to view the WINS servers in the console. Validating the cache

of WINS servers basically verifies the validity of records in its cache. This option can significantly delay the startup of the WINS server.

- **Server Status** This second node in the hierarchy simply displays the status of WINS servers, whether they are responding or not, as well as when the last database update was performed on the WINS server. You can also set the Server Status refresh intervals by right-clicking and going to Properties. The default is five minutes.
- **Server name/IP** These are the servers you have in your environment. Each WINS server shows an identical set of properties and controls. Right-clicking the server name will give you certain tasks you can perform on that server. Going to Properties, you will notice few configuration options. These options include:
 - Setting the duration of the Automatic statics refresh
 - Backing up the WINS database during shutdown
 - The time intervals at which WINS records will be renewed, deleted, or verified
 - You can also set WINS to run the verification process on its database records and validate the database consistency. Since it is a time-consuming and resource-intensive process, you can also configure the maintenance time needed to run, as well as the maximum number of records it will validate.
 - Logging options can also be configured under properties.

Under the Server node you have selected, the two other items in the hierarchy are Active Registrations and Replication partners. *Active Registration* shows you the records in the WINS database. You can also add manual static mappings here, as well as delete a record. *Replication partners* shows you the other WINS servers this WINS server is defined to exchange database information with. These partners can be configured as Push partners or Pull partners. In the Push partner setup, database information is pushed to the other WINS server at either a predefined time or at the record update option. In the Pull partner setup, the database information is pulled from other WINS servers at a specifically defined interval of time. Usually, both options are configured for the same WINS replication partners.

- **Database Scavenging** Records that are not validated during the database consistency check are marked for deletion and said to be tombstoned. This deletion process is known as database scavenging.

All these functions can also be performed manually.

Netsh WINS is the command-line counterpart to the WINS console. You can use Netsh WINS to perform all the tasks available in the WINS console from the command prompt on a computer running Windows Server 2003, as well as perform some additional tasks that can't be performed in the WINS console. To start Netsh WINS and access a specific WINS server, follow these steps:

1. Go to the command prompt. To start Netsh, type **netsh**. Notice the command prompt changes to netsh>.
2. Type **wins** to change the context to WINS. The command prompt now changes to netsh WINS>.
3. Type in the WINS server using its name or IP address, such as W2k08WINS or 192.168.11.2. Use a fully qualified domain name (FQDN) if the WINS server is in a different domain.
4. The command prompt changes to netsh WINS server>. You can now work with this particular WINS server. You can also select another WINS server to work with by typing the server followed by the server name or IP address without having to start over.

Configuring Replication Partners

With two or more servers in the environment, you can and should configure replication between them. The servers sharing their database information with other servers are called Replication partners. The two replication roles for WINS servers are the following:

- **Push partner** A server is said to be a Push partner when it informs other WINS server that updates to its database information are available to be exchanged.
- **Pull partner** A pull partner requests information updates from its replication partner.

Typically both the push and pull processes are used in a replication. The push client updates its replication partner regarding updates, while the pull partner requests the updates. By default, replication is enabled on WINS servers and both push and pull replication is configured on replication partners. By default, all replication is done using persistent connections to improve efficiency.

As replication is enabled and configured automatically, all that is required is to tell each WINS server of the other available WINS servers in the environment to

start replication. You can do this by using the automatic replication partner feature on a small network. Since this feature uses a broadcast to discover other WINS servers and can generate heavy broadcast traffic on a large network, you don't want to use this feature. Instead, you can assign replication partners manually.

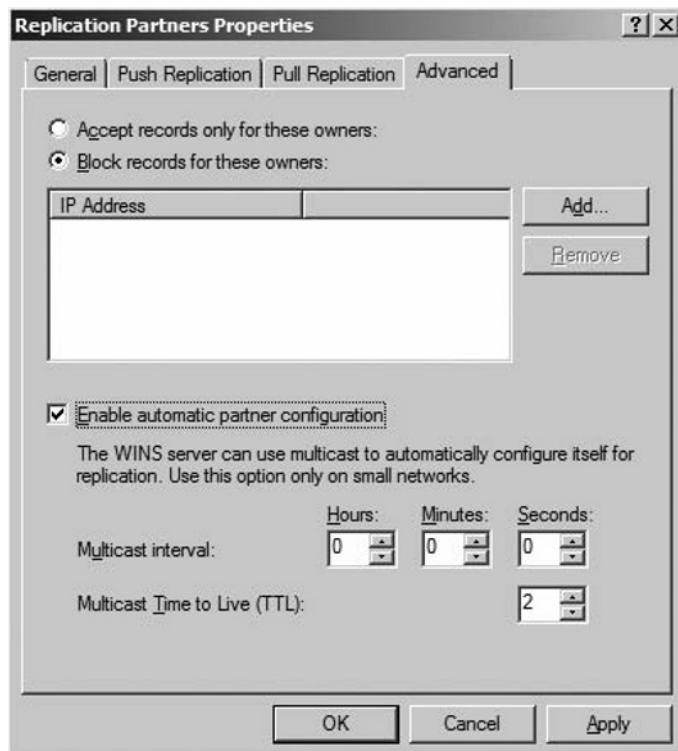
EXERCISE 1.6

CONFIGURING AUTOMATIC REPLICATION PARTNERS

Follow these steps to configure automatic replication partners:

1. Open the WINS console.
2. In the left pane, expand the server entry. Right-click the replication partner entry and select **Properties**.
3. In the **Replication Partner Properties** dialog box, select the **Advanced** tab, as shown in Figure 1.19.

Figure 1.19 Enable Automatic Replication



4. Select **Enable automatic partner replication**.
5. To set the interval between multicast broadcasts to the group of WINS servers, use the Multicast Interval options. The default interval is 40 minutes. Using these broadcasts, other WINS servers will know the availability of the WINS server you are configuring.

Note: Once your WINS server is discovered and registered as a partner with other WINS servers via multicasting, its record stays on its replication partners until you restart the WINS server or the WINS service. In a normal WINS server shutdown, it sends out the message to its replication partners that it is being shutting down and that its registration should be removed from their records.

6. You can specify how many hops these multicast broadcasts can go through before they are discarded. Use the Multicast Time To Live option for that. By default, these broadcasts can go through two routers.
 7. Click **OK**.
-

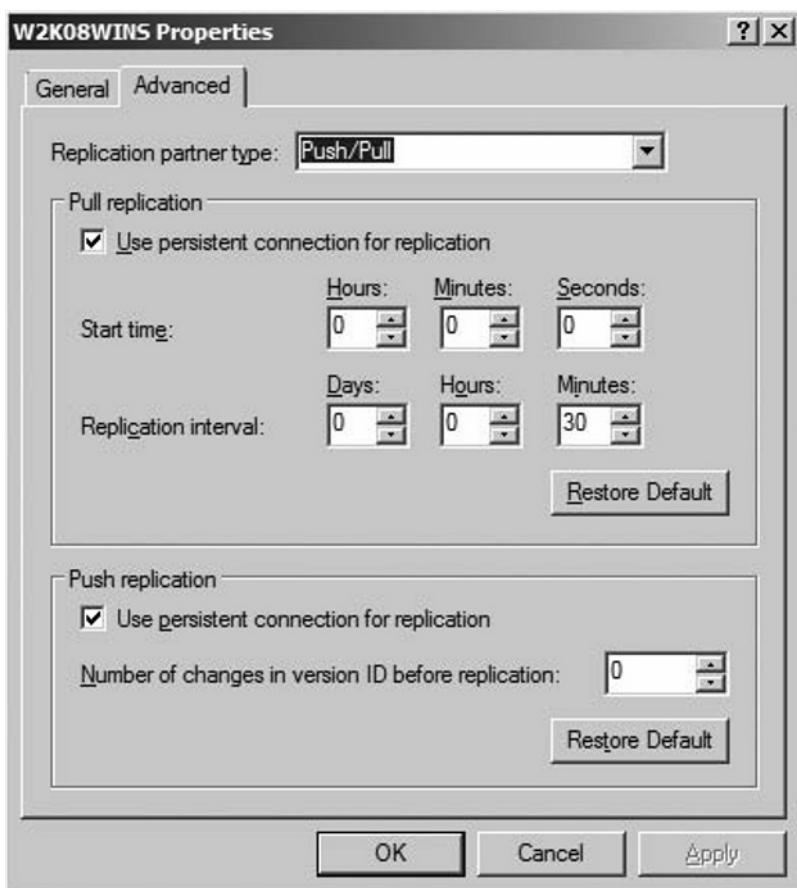
Specifying Designated Replication Partners

To use specific replication partners, do the following:

1. Start the WINS console.
2. In the left pane, expand the server node. Right-click the replication partner entry and select **New Replication Partners**.
3. In the **New Replications Partners** dialog box, enter the name or IP address of the WINS server you want to establish a replication partnership with.
4. Click **OK**.

At this point, you will see the WINS server listed in the WINS console. By default, the replication partners are configured with both push and pull. They are also configured to use persistent connections. This configuration is permanent and, unlike the automatic replication partner feature, it is not affected by the server restart.

You can view and change the replication settings by selecting the Registration Partners entry in the left pane and then double-clicking the replication partner in the details pane on the right. This displays the Properties dialog box of the replication partner as shown in Figure 1.20.

Figure 1.20 The Advanced Tab in WINS Properties

The configuration options shown in Figure 1.20 are the following:

- **Replication Partner Type** Push/Pull by default. Can be changed to just push or pull as well.
- **Pull Replication:**
 - **Use persistent connection for replication** This option when checked establishes a persistent connection for pull replication. This improves the performance since it reduces the time spent on opening and closing the connections.
 - **Start time** Sets the time when replication should begin.
 - **Replication Interval** Sets the replication frequency. This is 30 minutes by default.

- **Push Replication:**

- **Use persistent connection for replication** This option when checked establishes a persistent connection for push replication. This improves performance since it reduces the time spent on opening on and closing the connections.
- **Number of changes in Version ID before replication** Using this option, you can control after how many changes in the WINS database the replication should occur.

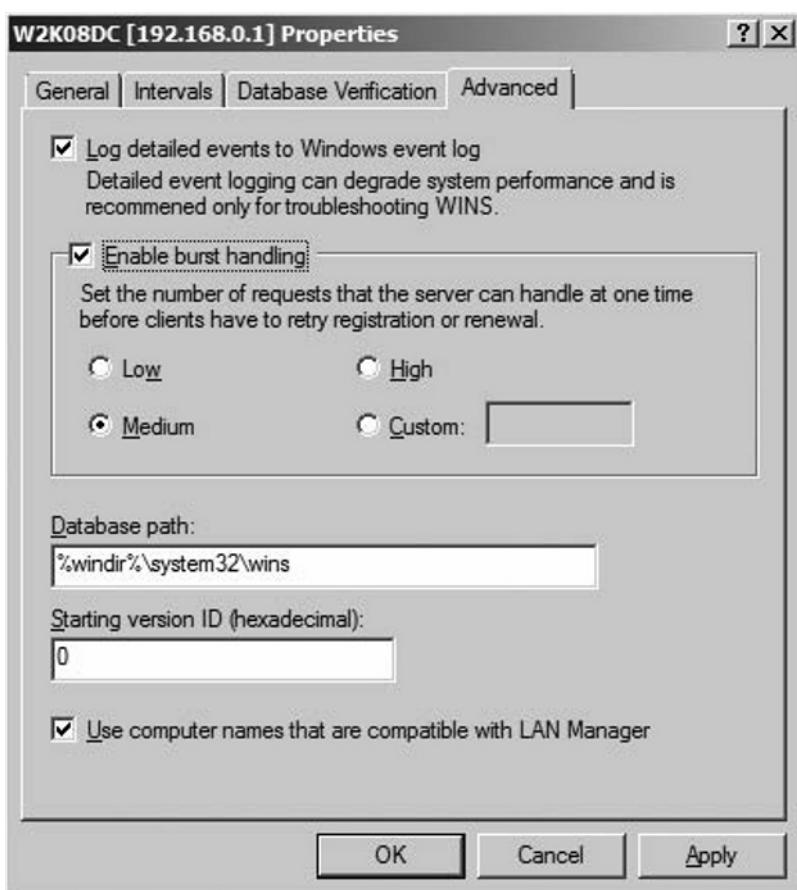
Maintaining WINS

Once replication partners have been set up, WINS is easy to maintain. Some configuration and maintenance tasks are noted in the following:

- Burst handling
- Active registrations and scavenging of records
- Maintaining WINS database

Burst Handling

Setting up appropriate burst handling allows WINS server to allocate the necessary resources and maintain queues for the settings you have defined. You should enable the burst handling of registrations if you have more than 100 clients in your environment. With the growth of your environment, review and reset the burst handling as appropriate. To get to the burst handling settings, go to the WINS console, right-click the **Server** node and go to **Properties**. You will see the settings in the Advanced tab, as shown in Figure 1.21.

Figure 1.21 Setting Burst Handling

Check the **Enable Burst Handling** box and select the appropriate setting from the following.

- **Low** For handling up to 300 registrations and name registration requests.
- **Medium** For handling up to 500 registrations and name registration requests.
- **High** For handling up to 1,000 registrations and name registration requests.
- **Custom** To set the custom threshold within a range of 50 to 5,000.

NOTE

Set up High or Custom values only if your network requires it. For example, if you set a threshold of 4,000, up to 4,000 requests can be queued at once. However, if your network requires only a queue with 500 name registration requests, much of your server resources will be wasted in maintaining an unnecessarily large queue.

NOTE: You can use the *netsh* command to view the configuration details of a WINS server by typing:

```
netsh wins server servername show info
```

where *servername* is the name or IP address of a WINS server.

```
WINS Database backup parameter
~~~~~  
Backup Dir :  
Backup on Shutdown : Disabled  
Name Record Settings(day:hour:minute)
~~~~~  
Refresh Interval : 004:00:00  
Extinction(Tombstone) Interval : 003:00:00  
Extinction(Tombstone) TimeOut : 006:00:00  
Verification Interval : 024:00:00  
Database consistency checking parameters :  
~~~~~  
Periodic Checking : Disabled  
WINS Logging Parameters:  
~~~~~  
Log Database changes to JET log files : Enabled  
Log details events to System Event Log : Enabled  
Burst Handling Parameters :  
~~~~~  
Burst Handling State : Enabled  
Burst handling queue size : 500  
Checking, Scavenging and Tombstoning Registrations
```

Scavenging Records

You can view the WINS database using WINS console. Expand the server node in the left pane, right-click **Active Registrations**, and select **Display Records**.

The Display Records dialog box appears. If you click Find Now without making any selection, it will display all the records in the database. You can also filter them by matching name patterns or IP addresses. When the records are displayed, you can manually tombstone a record by right-clicking a record and choosing **Delete**.

This action deletes the record from the current server as well as replicates the record to its replication partners as a tombstoned record.

WINS performs the scavenging process to delete tombstoned records automatically at predefined intervals. You can view the server statistics under the properties of a server to see the defined settings. Scavenging can also be initiated manually by right-clicking the server node in WINS console and choosing Scavenge Database. Scavenging the database can also be done at the command prompt by typing **netsh wins server ServerName init scavenge**, where *ServerName* is the name or IP address of the WINS server.

The LMHOSTS File

Just like the HOSTS file, the LMHOSTS file is a text file that provides NetBIOS name mapping to an IP address. This file is locally available on a computer. When a NetBIOS name resolution is required, NetBIOS clients will look at the LMHOSTS file before sending out the query to a WINS server or using a broadcast.

The path to this file is *systemroot:\WINDOWS\system32\drivers\etc*. This file has no extension. The entries in this file are not dynamic and are manually updated. Typically, you will not configure this file with entries since the file is specific to the computer you are working on. Hence, the entries will only apply to the computer where this file is updated. Also, if the host record is changed, the changes are not reflected automatically. The computer would have no information on updating the record and so it would keep mapping the IP address to a NetBIOS name since it is in the LMHOSTS file.

The following is a sample LMHOSTS file:

```
# Copyright (c) 1993-1999 Microsoft Corp.  
#  
# This is a sample LMHOSTS file used by the Microsoft TCP/IP for Windows.  
#  
# This file contains the mappings of IP addresses to computernames  
# (NetBIOS) names. Each entry should be kept on an individual line.
```

```
# The IP address should be placed in the first column followed by the
# corresponding computername. The address and the computername
# should be separated by at least one space or tab. The "#" character
# is generally used to denote the start of a comment (see the exceptions
# below).
#
# This file is compatible with Microsoft LAN Manager 2.x TCP/IP lmhosts
# files and offers the following extensions:
#
#      #PRE
#
#      #DOM:<domain>
#
#      #INCLUDE <filename>
#
#      #BEGIN_ALTERNATE
#
#      #END_ALTERNATE
#
#      \0xnn (non-printing character support)
#
# Following any entry in the file with the characters "#PRE" will cause
# the entry to be preloaded into the name cache. By default, entries are
# not preloaded, but are parsed only after dynamic name resolution fails.
#
# Following an entry with the "#DOM:<domain>" tag will associate the
# entry with the domain specified by <domain>. This affects how the
# browser and logon services behave in TCP/IP environments. To preload
# the host name associated with #DOM entry, it is necessary to also add a
# #PRE to the line. The <domain> is always preloaded although it will not
# be shown when the name cache is viewed.
#
# Specifying "#INCLUDE <filename>" will force the RFC NetBIOS (NBT)
# software to seek the specified <filename> and parse it as if it were
# local. <filename> is generally a UNC-based name, allowing a
# centralized lmhosts file to be maintained on a server.
#
# It is ALWAYS necessary to provide a mapping for the IP address of the
# server prior to the #INCLUDE. This mapping must use the #PRE directive.
#
# In addition, the share "public" in the example below must be in the
# LanManServer list of "NullSessionShares" in order for client machines to
# be able to read the lmhosts file successfully. This key is under
# \machine\system\currentcontrolset\services\lanmanserver\parameters\
# nullsessionshares
```

```
# in the registry. Simply add "public" to the list found there.  
#  
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE  
# statements to be grouped together. Any single successful include  
# will cause the group to succeed.  
#  
# Finally, non-printing characters can be embedded in mappings by  
# first surrounding the NetBIOS name in quotations, then using the  
# \0xnn notation to specify a hex value for a non-printing character.  
#  
# The following example illustrates all of these extensions:  
#  
# 102.54.94.97      rhino       #PRE    #DOM:networking   #net group's DC  
# 102.54.94.102     "appname"  \0x14"          #special app server  
# 102.54.94.123     popular      #PRE                #source server  
# 102.54.94.117     localsrv    #PRE                #needed for the include  
#  
# #BEGIN_ALTERNATE  
# #INCLUDE \\localsrv\public\lmhosts  
# #INCLUDE \\rhino\public\lmhosts  
# #END_ALTERNATE  
#  
# In the above example, the "appname" server contains a special  
# character in its name, the "popular" and "localsrv" server names are  
# preloaded, and the "rhino" server name is specified so it can be used  
# to later #INCLUDE a centrally maintained lmhosts file if the "localsrv"  
# system is unavailable.  
#  
# Note that the whole file is parsed including comments on each lookup,  
# so keeping the number of comments to a minimum will improve performance.  
# Therefore it is not advisable to simply add lmhosts file entries onto the  
# end of this file.
```

TCP/IP v4 and v6 Coexistence

TCP/IP is a suite of two protocols, Transmission Control Protocol (TCP) and Internet Protocol (IP). Internet Protocol (IP) is Layer 3-Network layer protocol and Transmission Control Protocol (TCP) is a Layer 4-Transport layer protocol.

It is expected that IPv4 and IPv6 will coexist and be supported for the foreseeable future. The primary change brought by IPv6 is a bigger address pool.

Features and Differences from IPv4

To a great extent, IPv6 is a conservative extension of IPv4. Most transport- and application-layer protocols need little or no change to work over IPv6—exceptions are application protocols that embed network-layer addresses. Applications, however, do need to make small changes to comply with IPv6. In the following list we discuss some of the differences between IPv4 and IPv6:

- **A larger address pool** The main feature of IPv6 that is driving adoption today is the larger address space: Addresses in IPv6 are 128 bits long versus 32 bits in IPv4. The larger address space avoids the potential exhaustion of the IPv4 address space without the need for Network Address Translation (NAT) and other devices that break the end-to-end nature of Internet traffic. It also makes administration of medium and large networks simpler, by avoiding the need for complex subnetting schemes. Subnetting will, ideally, revert to its purpose of the logical segmentation of an IP network for optimal routing and access. The drawback of the large address size is that IPv6 carries some bandwidth overhead over IPv4, which may hurt regions where bandwidth is limited (header compression can sometimes be used to alleviate this problem). IPv6 addresses are also very difficult to remember; use of the Domain Name System (DNS) is necessary.
- **Stateless Address Auto Configuration (SLAAC)** IPv6 hosts can be configured automatically when connected to a routed IPv6 network using ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local multicast *router solicitation* request for its configuration parameters. If configured suitably, routers respond to such a request with a *router advertisement* packet that contains network-layer configuration parameters. If IPv6 autoconfiguration is not suitable, a host can use stateful configuration (DHCPv6) or be configured manually. Stateless autoconfiguration is only suitable for hosts. Routers must be configured manually or by other means.
- **Multicast** Multicast is part of the base specifications in IPv6, whereas in IPv4, it was introduced later. IPv6 does not have a link-local broadcast facility; however, the same effect can be achieved by multicasting to the all-hosts group (FF02::1). Most environments, however, do not currently have

their network infrastructures configured to route multicasts. Multicasts on a single subnet will work, but global multicasts might not.

- **Link local addresses** IPv6 interfaces have link-local addresses in addition to the global addresses that applications usually use. These link-local addresses are always present and never change, which simplifies the design of configuration and routing protocols.
- **Jumbograms** In IPv4, packets are limited to 64KB of payload. When used between capable communication partners and on communication links with a maximum transmission unit (MTU) larger than 65,576 octets (65536 + 40 for the header). IPv6 has optional support for packets over this limit, referred to as jumbograms, which can be as large as 4GB. The use of jumbograms may improve performance over high-MTU networks.
- **Network-layer security** IPSec is the protocol for IP network-layer encryption and authentication and is an integral part of the base protocol suite in IPv6. This is unlike IPv4, where it is optional. However, it is not widely used at present.
- **Faster processing by routers** IPv4 has a checksum field that covers all of the packet header. Since certain fields (such as the TTL field) change during forwarding, the checksum must be recomputed by every router. IPv6 has no error checking at the network layer, but instead relies on the link layer and transport protocols to perform error checking, which should make forwarding faster.

Summary of Exam Objectives

Appropriate planning for computer names and name resolution methods is very important. Every organization should carefully define their strategy for their computers' naming scheme as well as their name resolution tools and techniques.

There are two types of naming conventions: internal names and external names. External names are public domain names and are controlled by a central registration body. You cannot use the same external domain name if it is already in use. External domains have root domains that are also predefined by the regulating body, and your public domain cannot be outside any of these root domains. Internal names are local to an organization and cannot be accessed by the public. Internal domain names are not regulated by Internet registrars.

Computers only understand numbers and communicate with each other through IP addresses. However, humans use computer names and, hence, need name resolution methods to relate computer names to their corresponding IP addresses. Two name resolution methods are used within Windows 2008 networks. Both of these methods are client/server protocols, meaning there is a client seeking information and a server responding to the request. These two systems are the Domain Name System (DNS) and Windows Internet Naming System (WINS).

DNS is a hierarchical or tree-like namespace. Internet domains are based on DNS. In DNS, the computer has a host name that can be up to 63 characters. DNS clients also have a fully qualified domain name (FQDN), which is their host name plus the domain suffix. The Windows Server 2008 DNS Server service includes some new features, such as globalnames zone, the read-only primary zone, background zone loading, global query block lists, link-local multicast name resolution (LLMR) for Vista clients, and full native support for IPv6 along with IPv4. DNS is required for Active Directory.

DNS servers can be configured with primary, secondary, stub, or globalnames zones. You can integrate zones with Active Directory where zone data synchronization takes advantage of Active Directory replication. DNS servers are configured to perform recursion by default where they send out a query to other DNS servers on behalf of the client to resolve the query. Dynamic updates is a feature where DNS clients can update their record on the DNS server. All computers from Windows 2000 and later can perform dynamic updates. The HOSTS file is a text file that can also provide DNS name to IP address resolution locally on a DNS client; however, all entries in this file are manual and static.

Unlike DNS, WINS has a flat namespace and does not use hierarchy, as in FQDN. WINS is used to resolve NetBIOS names to IP addresses. All Windows

systems have two names: a host name and a NetBIOS name. The NetBIOS name is limited to 15 characters in length. There is a hidden 16th character, which is used to limit the scope of communications for WINS clients.

In Windows Server 2008, WINS is considered a “feature” of the operating system. More than one WINS server should be installed for load balancing and redundancy. They synchronize their information via replication. Servers in WINS replication are called replication partners and are configured using push/pull methods, where push sends out the information and pull retrieves the information from its partner. LMHOSTS is a text file that can also provide NetBIOS name to IP address resolution locally on a computer; however, all entries in this file are manual and static.

Exam Objectives Fast Track

Windows Server 2008 Name Resolution Methods

- Windows Server 2008 networks use two name resolution methods, DNS and WINS.
- DNS uses host names, which can be up to 63 characters in length and also have domain names in front of them forming fully qualified domain names (FQDNs).
- WINS uses the NetBIOS protocol; NetBIOS names are limited to 15 characters in length. A hidden 16th character is used to define the NetBIOS communication scope for WINS clients.
- Internal names are local to an organization and cannot be accessed by the public. Internal domain names are not regulated by Internet registrars.
- External names are public domain names and are controlled by a central registration body. You cannot use the same external domain name if it is already in use. External domains have root domains, which are also pre-defined by the regulating body, and your public domain cannot be outside any of these root domains.

Domain Name System

- Windows Server 2008 DNS server service includes some new features, such as globalnames zone, read-only primary zone, background zone loading, global query block list, link-local multicast name resolution (LLMR) for Vista clients, and full native support for IPv6 along with IPv4. DNS is required for Active Directory.

- A DNS query is made when a DNS client seeks information from a DNS server. The DNS server receiving the DNS query checks its local database to resolve it. If there is no record in its database, the DNS server will forward the request to an authoritative DNS server. The DNS query process proceeds as follows, and at whichever step the query is resolved, a response is then sent to the client with the answer, thus stopping the process:
 - The DNS client's Local Resolver cache
 - The HOSTS file
 - The DNS server's database and cache
 - The DNS server to other DNS servers' databases if recursion is enabled on the DNS server. It is enabled by default.
 - If WINS lookup is enabled, the DNS server can query WINS to resolve the name.
- Forward lookup queries and reverse lookup queries are used. Forward lookup queries resolve host names to IP addresses. Reverse lookup queries resolve IP addresses to host names.
- An authoritative DNS server for a domain will contain all the resource records part of the domain for which it is authoritative. DNS servers also store resource records in their cache when they resolve a query for a DNS client. A few types of host records are supported by the Windows Server 2008 DNS Server service, such as A (IPv4 host), AAAA (IPv6 host), CNAME (Alias), MX (mail exchanger), NS (Name Server), PTR (Pointer), SOA (Start of Authority), SRV (service location).
- A zone is a portion of a namespace for which an authoritative server has full information and control. These include primary, secondary, stub, Active Directory-integrated, and globalnames zones. Primary zones contain a master read-write copy, while secondary zones contain a read-only copy and get their information from the primary zone. The zone transfer takes care of zone replication. In Active Directory-integrated zones, replication is taken care of by Active Directory.

DNS Server Implementation

- ☒ The DNS Server service on Windows Server 2008 can be installed in two ways. It can be installed by going to the Server Manager console and adding the role. It can also be installed when you are first installing Active Directory via *dcpromo*.
- ☒ Zones can be created by right-clicking and adding the zone. There is an option to integrate a zone with Active Directory. Only those DNS servers that are domain controllers as well can host the Active Directory-integrated zones. If the zone is Active Directory-integrated, SRV records for domain controllers, global catalog servers, and PDC Emulator are automatically created.
- ☒ Secure dynamic updates allows subsequent DNS updates only by a client that originally registered/created the record in the DNS server. In non-secure updates, any machine can update the record regardless of who first registered it. These settings can be configured in zone properties. If DHCP is configured for dynamic updates, PTR records of the clients are automatically updated as well.
- ☒ The Aging and Scavenging feature provides a means of cleaning out old outdated records or setting how long will they be valid. It can be applied at either the Server level or the Zone level. A checkbox needs to be selected to enable it.
- ☒ On DNS client, you must set at least a host name, primary DNS suffix, and a DNS server. You can also set the following under the DNS tab by going to TCP/IP properties and clicking the Advanced button:
 - ☒ The DNS servers list in order of priority
 - ☒ The DNS suffix search order
 - ☒ The connection-specific DNS for each network adapter
 - ☒ The dynamic DNS update behavior
- ☒ WINS lookups for DNS server can be enabled in zone properties under the WINS tab.
- ☒ The HOSTS file is a manual text file that provides DNS name mapping to IP addresses. The path to this file is `systemroot:\WINDOWS\system32\drivers\etc`. This file has no extension.

Windows Internet Naming Service (WINS)

- WINS provides mapping for NetBIOS names to the associated IP addresses. NetBIOS names are limited to a maximum length of 15 characters.
- NBT is NetBIOS over TCP/IP and is used to get around NetBIOS non-routability.
- Node types are methods that clients use to resolve NetBIOS names. It can be set up via the Registry or via DHCP. The node types are:
 - B-node (broadcast)*
 - P-node (peer-peer)*
 - M-node (mixed)*
 - H-node (hybrid)* Reverts to b-node if it cannot resolve the name.
This is the default for Windows 2000, XP, Windows 2003, and Windows Server 2008 client machines that are configured with WINS.
- In Windows Server 2008, WINS is installed in two ways. One, by going to the Server Manager console and adding a feature. And two, by going to the Control Panel, clicking Programs and Features, clicking Tasks, and selecting Turn Windows Feature Off or On.
- To configure WINS, go to **Start | Administrative Tools | WINS**. This opens up the WINS Management Console.
- If there is more than one WINS server, replication partners are set to configure WINS database synchronization. These partners can be configured to push or pull (or both) at a set amount of time or after a certain number of updates in the WINS database. This is done by going to the Replication Partners option under the Server node in the WINS Console.
- Automatic WINS partner configuration can be enabled under Replication Partner Setup in the Advanced tab; however, it is meant only for small networks since it uses multicast.
- You can enable the use of persistent connection for replication by going to Server Properties in the Advanced tab.

- The scavenging of stale or tombstoned records can be set to predefined intervals or can be done manually.
- The LMHOSTS file is a manual text file that provides NetBIOS name mapping to IP addresses. The path to this file is systemroot:\WINDOWS\system32\drivers\etc. This file has no extension. Typically, this file is not configured with any entries.

IPv4 and IPv6 Coexistence

- Most transport- and application-layer protocols need little or no change to work over IPv6; exceptions are application protocols that embed network-layer addresses.
- The main feature of IPv6 that drives adoption today is the larger address space: Addresses in IPv6 are 128 bits long versus 32 bits in IPv4.
- IPv6 interfaces have link-local addresses in addition to the global addresses that applications usually use. These link-local addresses are always present and never change, which simplifies the design of configuration and routing protocols.

Exam Objectives

Frequently Asked Questions

Q: What are the two name resolution methods I can use within Microsoft Windows Server 2008 networks?

A: You can use DNS or NetBIOS or both.

Q: How can I differentiate an internal domain name from an external domain name?

A: Internal names are not accessible by the public and are not registered in the Internet domain naming authority.

Q: Do I need to install the DNS client service on my computers running Windows XP?

A: No. The DNS client service is installed by default with Windows operating systems.

Q: Can I install Active Directory without DNS server?

A: No. DNS is required for Active Directory

Q: I am planning to use Active Directory-integrated zones. Can I make a Windows Server 2008 that is not a domain controller a primary DNS server?

A: No. If you are planning to install an Active Directory-integrated zone, a primary DNS server must be an Active Directory domain controller since only domain controllers have master read-write copy.

Q: Does Windows 2008 support IPv6?

A: Yes. IPv6 is fully supported by Windows Server 2008, along with IPv4.

Q: I am using Windows Vista. Does my computer have a NetBIOS name?

A: All Windows operating systems have a NetBIOS name.

Q: I have just installed Windows 2008 Server. Do I need to give it a NetBIOS name?

A: Yes. You must assign a host name and a NetBIOS name.

Q: How long can a NetBIOS name be?

A: Fifteen characters.

Q: What is the default node type of all operating systems after Windows 2000 configured with WINS?

A: H-node (hybrid). It reverts to b-node if it cannot resolve the name. This is the default for Windows 2000, XP, Windows 2003, and Windows Server 2008 client machines that are configured with WINS.

Q: Can I install WINS on the same server where the DNS Server service is also installed in Windows Server 2008?

A: Yes. You can install WINS on the same Windows Server 2008 system, along with the DNS Server service.

Q: How can I view the NetBIOS cache on the WINS client?

A: By going to the command prompt and typing *nbstat -c*.

Q: How can I clear the NetBIOS cache on a WINS client?

A: By going to the command prompt and typing *nbstat -R*.

Q: What command line tool can I use to configure a WINS server?

A: *netsh*. You can use the *netsh* command to view, modify, or troubleshoot the WINS configuration.

Q: My company has a network spanned across multiple physical locations. Should I use WINS automatic partner configuration?

A: No. WINS automatic partner configuration uses multicast and is only meant for small networks.

Self Test

1. Steve is an IT administrator who recently joined an electronics manufacturing company. His company has decided to use computer names of 16 characters. One day, a user complains that she is not able to reach a Windows 2008 server named memberserver120A. While troubleshooting, Steve notices there are two names for the Windows 2008 Server in computer properties, a 16-character name, memberserver120A, and a 15-character name, memberserver120. What is this 15-character computer name?
 - A. This is a native computer name.
 - B. This is a NetBIOS name.
 - C. This is fully qualified domain name.
 - D. This is a secondary host name.
2. What is the root domain name of a namespace in FQDN alpha.nsoftad.internal.?
 - A. alpha
 - B. nsoftad
 - C. internal
 - D. There is no root domain in FQDN.
3. You are the network administrator for your company and have upgraded all your computers to Microsoft Windows Server 2008. Client computers are running Microsoft Windows Vista. The DNS service has been installed on a member server within the company domain. You want to provide fault tolerance for your zone so that name resolution can still continue if the DNS server goes offline. You plan to add another DNS server to the domain, but need to configure the new DNS server role in the appropriate role. What should you do?
 - A. Configure the new server as a secondary DNS server.
 - B. Configure the new server as a master name server.
 - C. Configure the new server as a caching-only server.
 - D. Configure the new server as a DNS forwarder.

4. Connor is an IT manager of a food supply company. He has upgraded his company's domain controllers to Windows Server 2008. The company is planning to open a new remote branch that will be connected to the corporate office via a 128-kbps WAN link. Connor wants to install a DNS Server service in the branch office to limit the DNS query traffic going over the slow WAN link and to improve performance; however, he does not want to configure any zones on that DNS server or install a domain controller. What shall he do?
 - A. Install a secondary DNS server in the branch office.
 - B. Configure a DHCP server to provide the zone configuration.
 - C. Install a caching-only DNS server in the branch office.
 - D. Connor cannot install a DNS server without zones.
5. What steps does a DNS client take before it sends out the query to a DNS server for resolution?
 - A. A local resolver cache is checked.
 - B. The HOSTS file is checked.
 - C. It broadcasts to a local subnet.
 - D. It contacts the WINS server.
6. Steve is a Windows administrator of a small printing company. The company has a Windows 2008 domain Qprint.net and his company recently purchased Microsoft Exchange Server 2007. He has installed the Exchange server, mailsrv, but he can't receive any e-mails. What must Steve do to ensure that e-mails are received to his Exchange Server?
 - A. Update the PTR record on the ISP DNS for Exchange.
 - B. Create the MX record on the ISP DNS for Exchange.
 - C. Update a record on the ISP DNS for Exchange.
 - D. Create an SRV record for Exchange Server.
7. Your company has decided to upgrade your Windows 2003 network to Windows Server 2008. You start with the servers and complete the migration of the Windows 2003 servers and services to Windows Server 2008 without trouble. The DHCP and WINS servers provide their services properly with few issues. You leave the WINS configurations and DHCP scopes as they were before. Your

Windows 2008 DHCP server was configured to deliver the default gateway, but the DNS servers were manually configured on clients. You have your support technicians begin the process of upgrading the Windows XP workstations to Windows Vista. During the process, they notice there is an option to obtain DNS automatically, and they select that option in order to match the Obtain An IP Address Automatically option. When they attempt to browse the Internet, they can't locate any resources. What is the most likely cause of the problem?

- A. The technicians need to restart the machine for the changes to take effect.
 - B. The DHCP server does not have the DNS information.
 - C. The DHCP configuration from the Windows 2003 server that was migrated will not properly serve the Windows Vista workstations.
 - D. You need to manually remove the old DNS entries from the Advanced menu tab.
8. Shannon's company has a Windows Server 2008 domain. All of her company's servers run Windows Server 2008 and all of the workstations run Windows Vista. The company's DHCP server is configured with the default settings and all of the Windows Vista machines are configured as DHCP clients with the default DHCP client settings. Shannon wants to use DNS dynamic updates to automatically register the host record and the PTR record for all of the company's workstations. What must she do to accomplish her goal?
- A. Nothing. The default settings are sufficient.
 - B. Configure the DHCP server to always Dynamically update DNS and PTR records.
 - C. Configure the DHCP server to Dynamically update DNS and PTR records only if requested by the DHCP clients.
 - D. Configure the workstation to use dynamic updates.

9. Jasper is a systems administrator of a marketing company. The company has a domain called nsoftad.com and support.nsoftad.com. All servers are running Windows 2008. Jasper has a delegated support.nsoftad.com to another DNS server; however, he wants to ensure that whenever a new authoritative name server is added for support.nsoftad.com zone, the DNS server for nsoftad.com is notified. What should he do?
 - A. Configure a stub zone on the DNS server within the parent domain.
 - B. Using the Name Servers tab from the support.nsoftad.com zone, configure the DNS server to notify the DNS server in the parent domain of any changes.
 - C. Configure a DNS server within the nsoftad.com zone to be a secondary server to the support.nsoftad.com zone.
 - D. Configure all zones to store information within Active Directory.
10. Steve is a network administrator of a large company. All of the company's ten domain controllers and 50 member servers are running Windows Server 2003. The company is planning to retire WINS servers and has moved to DNS for name resolution; however, there are a few legacy applications requiring WINS-like name resolution without using FQDN. Steve has heard about the new feature of globalnames zone in Windows Server 2008 to address this issue. He upgraded one of his domain controllers to Windows Server 2008. However, when he tries to configure the globalnames zone, he is unable to do so. What could be the reason for this? (Choose all that apply.)
 - A. All the domain controllers need to be running Windows Server 2008.
 - B. The forest level is not set to Windows Server 2008.
 - C. All the member servers need to be running Windows Server 2008.
 - D. There is no such feature as the globalnames zone.

Self Test Quick Answer Key

- | | |
|------------|-------------|
| 1. B | 6. B |
| 2. C | 7. B |
| 3. A | 8. A |
| 4. C | 9. A |
| 5. A and B | 10. A and B |

Chapter 2

MCITP Exam 647

Designing a Network Access Strategy

Exam objectives in this chapter:

- Network Access Policies
- Remote Access Strategies
- Working with Perimeter Networks
- Server and Domain Isolation

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

Designing and implementing an enterprise network access strategy has always been a significant challenge for network administrators given the many different ways users and devices interact with the network, each with its own configuration and security concerns. This diversity has made it nearly impossible to develop a single set of policies that could be enforced and configured centrally across the enterprise. Likewise, the monitoring and auditing of these policies was spread across different management consoles, creating an organizational burden on the network administrators.

Windows Server 2008 has united these technologies into an enterprise platform that centralizes the configuration, management, auditing, and administration of network access policies. This unification of technologies brings together some of the most often misunderstood parts of the server platform into a single powerful toolset, allowing the network administrator to not only control security in data transfer, but also the workstation requirements for participation on the network.

In addition to significant improvements in existing technologies, Windows Server 2008 introduces a number of new technologies to provide improved network security when interacting with client computers, such as more secure VPN tunneling and better isolation between external networks and internal corporate resources.

This chapter shows how to develop and implement a network access strategy for an organization's network and servers using the tools included with the Windows Server 2008 operating system.

Network Access Policies

Defining an appropriate network access strategy forces the network administrator to deal with one of the fundamental paradoxes of network access management—users expect to be able to work anywhere and any time, but also need their data to be secure. This means that controlling network access is more than just controlling permissions; it means being able to provide secure access to the data and protect the network environment even when the network administrators are not in control of the workstations and remote networks themselves. Clearly, this is a larger problem that requires a broader approach to security.

Using Windows Server 2008, a network administrator is able to define not only who should get access to the data but also how that access is provided and what criteria client devices must meet to participate in the communication. This means that complete control over Authentication, Authorization, and Auditing (AAA) must be defined for all client request types (see Table 2.1).

Table 2.1 Understanding Authentication, Authorization, and Auditing

| AAA Process | Definition |
|----------------|--|
| Authentication | This is the process where a user asserts its identity against the directory or local machine with a known credential to verify their identity. Examples of this are authentication against Active Directory, with a user or computer certificate, or through Kerberos. |
| Authorization | This is the process where an authenticated user requests access to a network resource and the authentication token is validated against the object's security settings to determine what actions that user can perform on the object. This may take the form of matching Access Control Entries in an Access Control List, validating against a database, or even a custom authorization implementation in an application. |
| Auditing | This is the logging and documentation of the Authentication and Authorization requests and the outcomes of each of these transactions. The method of auditing and the detail kept is determined by the type of access requested and technology involved. Windows Server 2008 has many different auditing methods covering file access, network access, and directory access. |

Network Access Methods

Just as important as the control of the access method is the nature of the network access itself. Each different type poses its own level of risk and specific challenges to the security of the network. A complete network access strategy is not a one-size-fits-all plan, but defines what access methods are valid and what criteria each must meet to participate on the network.

The point of greatest risk on a network is in the interface with the outside world where another machine is requesting access to internal data. In a tightly controlled corporate network, these requests are done under relatively controlled circumstances. As additional entry methods are allowed, the network has to assume the risk posed by these external systems, including any security issues these might have. This means your network is only as secure as the weakest link in the system. For instance, having excellent antivirus protection only mitigates some of the risk if you routinely allow machines with no antivirus protection to connect to your network.

NOTE

It is important to remember that the network is only as secure as its weakest link. It only takes one point of entry to allow potentially dangerous programs into your network, or worse, to send private corporate data outside it. For this reason, it is crucial to control network access at each entry point. Every connection to the network is a potential point of compromise and should be regarded as untrusted until proven otherwise!

Local Network Access

Devices that are directly connected to the network as part of the corporate network are the easiest to directly control, but they also will generally have the most access to network resources. These are not without challenges, however, since they often will be heavily reliant upon network resources for their function and small disruptions here can directly impact the business.

- **Wired Workstations** Traditionally, very little has been done to control the network access that wired workstations have to the enterprise. These are usually considered to be part of the infrastructure and are given a high level of trust since group policies and security settings provide some level of security.

In practice, wired workstations often will have security settings disabled given that exceptions are made for individuals and third-party applications that don't follow the corporate security standards. This is further compounded by niche applications and often uncontrolled Internet access.

- **Wireless Workstations** While wireless workstations directly participate in the network, they bring their own set of challenges to the table. These are often laptops that roam between corporate and private networks and may not be subject to the same policies and security controls as wired workstations. Control over Windows Updates, antivirus software, and firewall settings are usually not as tightly controlled and may even be disabled.

The very nature of the wireless network link also creates inherent security concerns. While these are usually considered to be directly connected, the fact that data are transferred over the air means that additional encryption protocols must be introduced to protect from electronic eavesdropping or system compromise.

Remote Network Access

Unlike local network access methods, remote access provides network access to workstations and devices that are not part of the corporate network and are usually completely outside of the administrator's control. These workstations can connect through a variety of methods requiring planning and security policies for each valid method.

- **Terminal Services** These clients connect to either a Terminal Services Gateway or a Terminal Server and are presented with either a terminal-enabled application or a remote desktop. During this terminal session, the remote workstation is connected directly with the network, and potentially confidential corporate data are transferred between the server and workstation. Thus, care must be taken to protect the corporate network, as well as ensure that all data transferred are secure.
- **Virtual private network (VPN)** Remote machines with Internet access can make VPN connections with Windows Server 2008 machines by creating a secure tunnel between the workstation and a VPN endpoint. This is particularly dangerous since this bridges the remote workstation directly into the corporate network.
- **Dial-up access** Similar to the VPN scenario, workstations can also dial directly into a server running the RRAS role over ISDN or standard telephone lines. This brings the workstation directly into contact with the corporate network.

It is important to carefully design which access methods you will employ to let users connect to your network and develop a specific policy for each to control both the security of the connection as well as the workstation security requirements that must be in place for network membership.

RADIUS Server

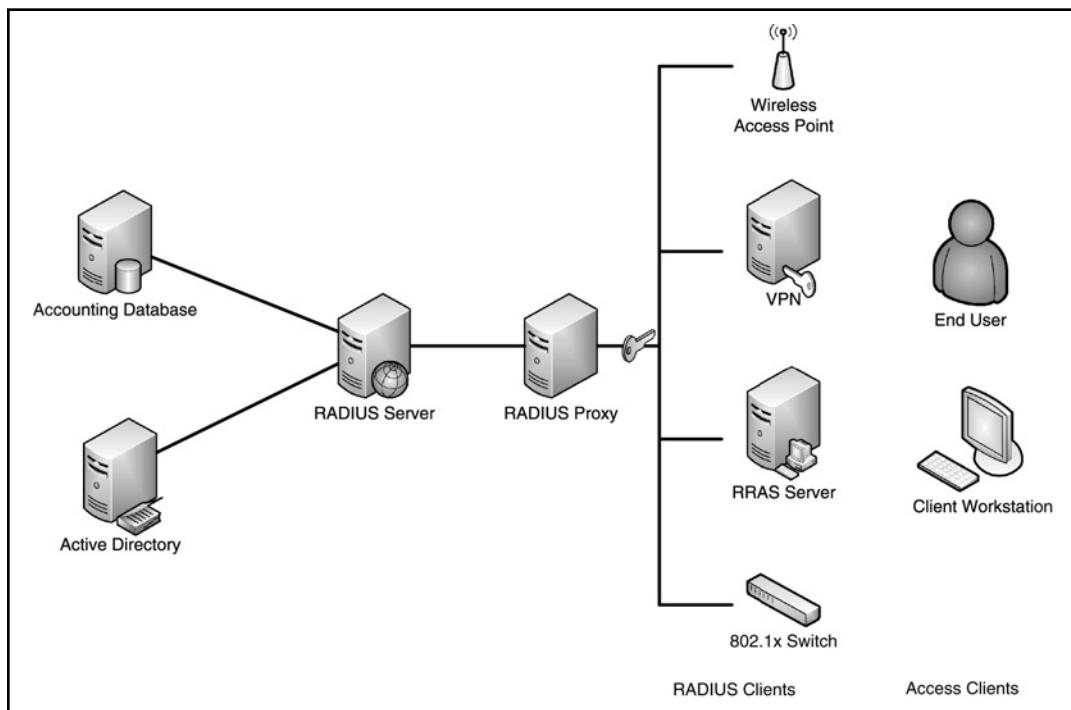
The Remote Authentication Dial-In User Service (RADIUS) is a suite of technologies that work together to provide a complete end-to-end AAA solution. This is an industry-standard protocol (described in RFC 2865) that has been implemented on a number of hardware and software platforms and is one of the core network administration protocols that exists in almost all networks in one form or another.

EXAM WARNING

Radius is an industry-standard protocol that, by default, listens for traffic on UDP/1812 for authorization and UDP/1813 for accounting. Over the years, the standards have changed, but the Windows 2008 implementation of RADIUS will listen on the legacy ports UDP/1645 and UDP/1646 as well.

Normally, when computers attempt to authenticate with a network, they are directly accessing the authenticating servers, making their requests against the authentication source. This can work well if you have a high level of trust that the machine making the request is healthy and poses little risk, but as the network becomes increasingly distributed, this assumption might no longer be true. Traveling laptops, wireless connections, dial-up users, and VPN users can make access requests from almost anywhere, and the machines used to make these connections can oftentimes roam between a number of different home and corporate networks—not to mention the occasional coffee shop.

RADIUS provides an additional level of abstraction between these requesting clients and the back-end authentication infrastructure that is responsible for the account validation. This means that the end-user workstation (Access Client) talks only to a RADIUS Client that is responsible for making the authorization request, as well as controlling the access. This RADIUS Client is part of the enterprise RADIUS infrastructure and is often secured with shared secrets (passwords) or certificates to ensure that the communication is secure. The RADIUS Client can also secure communication with the workstation to ensure the authentication information is never transmitted across the wire in an unencrypted fashion (see Figure 2.1).

Figure 2.1 The Enterprise RADIUS Infrastructure

RADIUS Components

RADIUS is not tied to specific clients or servers and can be used to provide AAA to a broad range of network devices and applications. To accomplish this, a number of different components go into building a RADIUS solution.

- **RADIUS Access Clients** Access Clients are the end-point client machines that are requesting AAA services from the RADIUS system. These are simply machines that would like to use the network and must request access and provide credentials.
- **RADIUS Clients** Unlike Access Clients, RADIUS Clients are infrastructure devices that are associated with the RADIUS infrastructure and are the control devices that permit or deny traffic on the network. These are explicitly registered in the RADIUS server by IP address as being allowed to request authorization on behalf of the Access Clients. In practice, these can be RRAS components of Windows 2008 Server, Wireless access points, infrastructure switches, network routers, or RADIUS proxy servers.

The Client is also responsible for handling the response that the server sends back for the authorization request. If the network access is denied or if information is sent back changing the 802.1q VLAN tagging, the Client must respond to this, assigning the appropriate access to the RADIUS Access Client.

NOTE

It is important to differentiate between RADIUS Access Clients and RADIUS Clients. Access clients cannot talk directly to the RADIUS servers, whereas the RADIUS Client is responsible for mediating this communication and handling the response.

- **RADIUS Proxy** In an environment that is highly distributed or that will handle a large number of RADIUS requests, it is often important to control the network flow of these requests to ensure they are appropriately delivered and that this communication is secured as necessary. RADIUS proxy servers act as these aggregation points, forwarding RADIUS requests to appropriate servers and routing the responses back to the RADIUS Clients.
- **RADIUS Server** The RADIUS Server is the central hub of RADIUS communications accepting authorization requests from the RADIUS Clients, establishing authentication credentials with the Authentication Database, communicating request responses with the clients, and maintaining the Accounting database.
- **Authentication Database** Upon implementation, RADIUS in NPS is able to connect to a number of different Authentication Databases to validate authorized access. Out of the box, it can integrate with Active Directory, an NT 4.0 domain (NTLM), or a local Security Account Manager (SAM Database). Other providers can also be used, but these require additional integration and planning.
- **Accounting DataStore** RADIUS is capable of storing detailed Accounting information from the RADIUS Client. This information tracks the authentication requests and the response back from the server. It also tracks the information passed back in the RADIUS response that might be used to assign different RADIUS attributes, such as VLAN or other control information.

Using NPS under Windows 2008, you have two different options for the accounting database. By default, this is stored in a standard log file.

Traditionally, this has worked well, but with the expanded authorization methods implemented to track health policies and wired access, this will grow faster than ever and may easily become unmanageable. You can also choose to store the Accounting DataStore in SQL 2005 to provide better scalability, centralized storage, and faster response than could be gotten from the standard log.

Network Policy and Access Services

Several new technologies have been introduced in Windows Server 2008 to support the management of network access policies through the Network Access Protection (NAP) Server components. NAP allows a network administrator to define base criteria that clients will have to meet when participating in network communications. Client workstations that do not comply with the network policy will be denied access to the network or will be assigned to a network segment that has limited functionality—usually only the servers and resources that a workstation would need to bring itself into compliance.

Head of the Class...

Security on Servers

It is easy to control the security on server machines in your network because you control all of the pieces. You have the opportunity to plan the implementation, test configurations, and audit the security of individual components. Workstations, on the other hand, are out in the wild—users browse the Internet, install applications, share files, and bring applications in from the outside. These are the weakest link in the network security and can be the hardest to control.

Traditionally, you would lock the workstations down, configure the firewall settings, install antivirus software, and apply GPOs to control this risk. The problem with this is that it relies on the technology working flawlessly to provide security. So, in a large environment with varied workstation configurations and user rights, it is easy for exceptions to occur.

NAP forces the workstation to prove it is complying with the network policy before it is granted access to network resources. This is an affirmative policy that relies on the state of the workstation rather than an assumption of compliance.

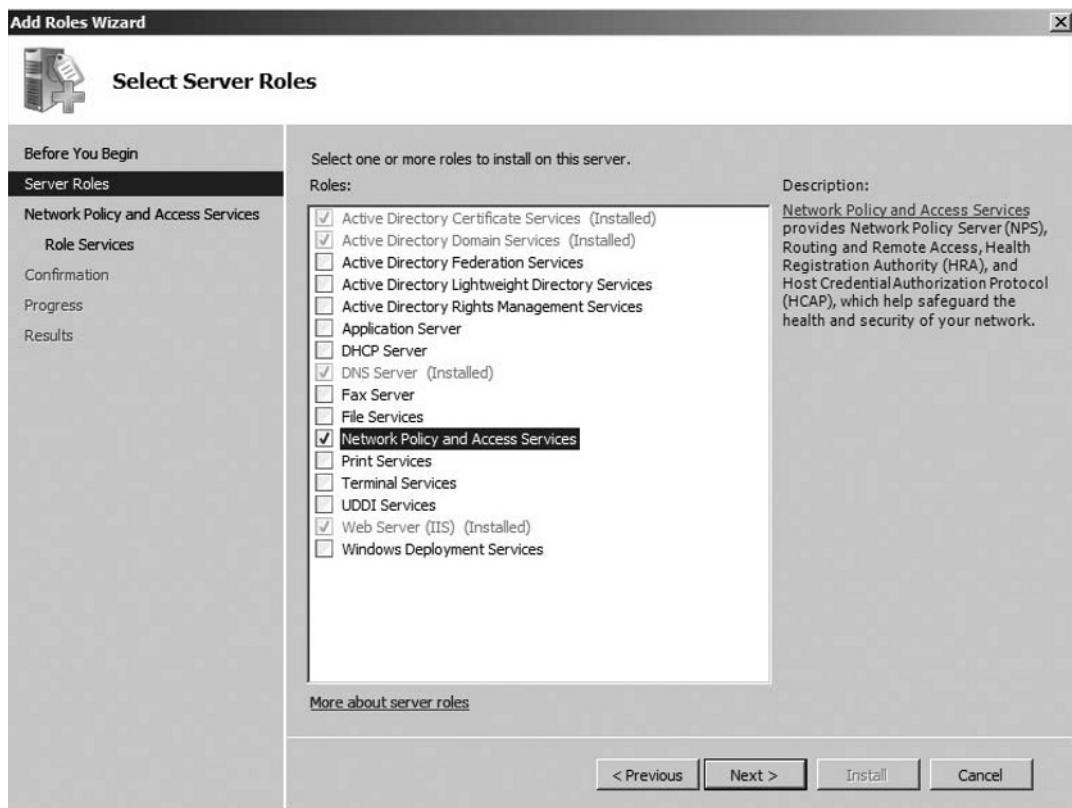
EXERCISE 2.1

ADDING THE NETWORK POLICY AND ACCESS SERVICES ROLE

This exercise assumes that Windows Server 2008 is running in a domain environment and that an Enterprise Certificate Authority has already been deployed.

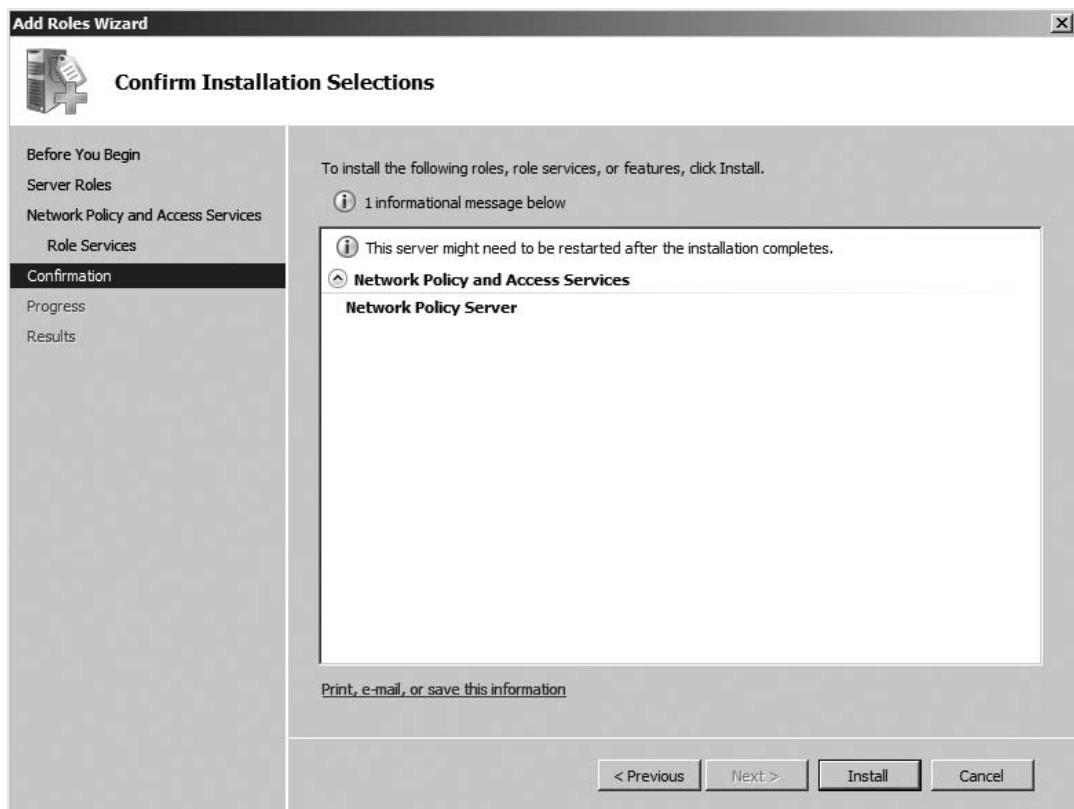
1. Open Server Manager by choosing Start | Administrative Tools | Server Manager.
2. Right-click Roles and choose Add Role.
3. Mark the checkbox for **Network Policy and Access Services** (see Figure 2.2) and then click **Next**.

Figure 2.2 Selecting Server Roles



4. Click **Next** to begin the configuration process.
5. Check the box for **Network Policy Server** and click **Next**.
6. Validate that the selected options are correct (see Figure 2.3) and then click **Install**.

Figure 2.3 Confirming Installation Selections



7. Click **Close** once the installation is complete.

TEST DAY TIP

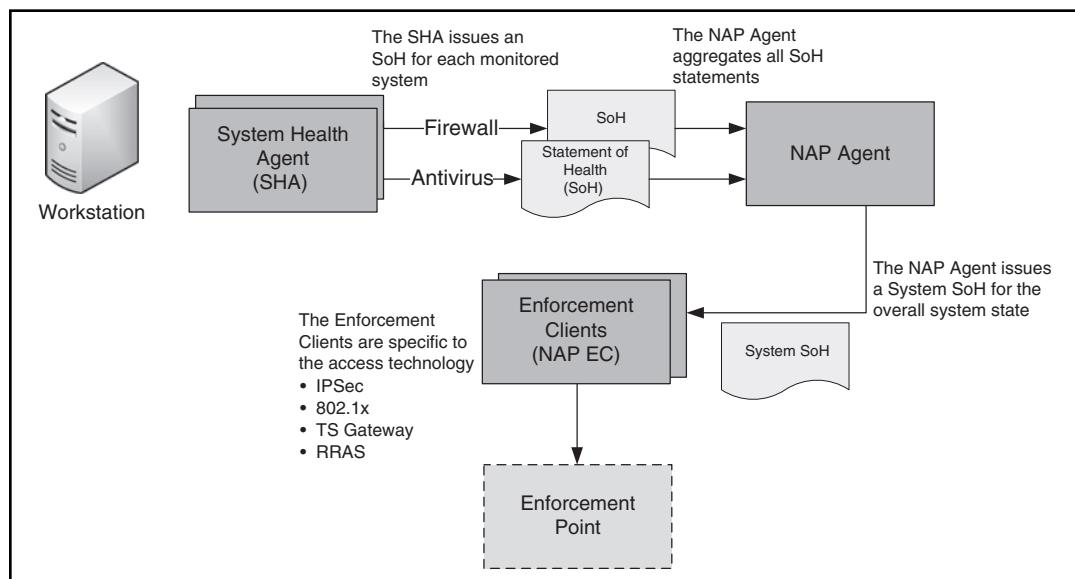
NAP is only supported on servers running Windows Server 2008 and clients running Windows Server 2008, Windows Vista, or Windows XP (SP3 or later) natively though the Microsoft API enables third-party vendors to build NAP-aware applications that will participate in the NPAS infrastructure.

NAP Client Components

Full implementation of NAP requires the participation of many different components, each playing a vital role in the evaluation of client health and the authorization of that client to participate on the network. Not surprisingly, the client has a vital role to play in the NAP communication and must be able to both assert its validity on the network and also interpret and abide by the response from the server.

In order to interface with the server components, the client must implement a number of interfaces and be able to collect appropriate information about itself and the software it runs. These components interact with one another to generate a statement of health (SoH) that the server can use to validate against its internal rule set and then grant permission for the client to participate on the network (see Figure 2.4).

Figure 2.4 NAP Communication on a Network



- **System Health Agent (SHA)** This component is responsible for evaluating the status of individual subsystems and applications running on the workstation. A separate SHA will be running for each monitored system to provide inspection into the running status of that service. The SHA is responsible for generating Statement of Health (SoH) declarations and routing them to the NAP Agent.

It should be noted that the SHA is only responsible for examining the current status on the client and generating the SoH; the evaluation of this

information is done on the server platform by the matching System Health Validator (SHV). Third parties might choose to implement their own System Health Agents to provide specific information about custom services like antivirus, anti-spyware, anti-spam, and other services.

The SHA will also accept Statement of Health Response (SoHR) declarations from the SHV that will provide remediation to a noncompliance state so the workstation can mitigate any outstanding fault and apply for access to the network again.

NOTE

Microsoft provides the Windows System Health Agent (WSHA) as a built-in agent to produce Statements of Health covering the Windows firewall, Windows Update, and the presence of enabled antivirus and anti-spyware software.

- **Statement of Health (SoH)** Each SoH is a declaration of the current running state of the client machine as evaluated by the SHA.
- **NAP Agent** This agent is responsible for collecting all of the SoH assertions sent to it by the SHAs running on the client workstation. The NAP Agent then aggregates this into a System Statement of Health (System SoH) that will be used to represent a holistic picture of the client's health status.
- **NAP Enforcement Clients (NAP EC)** This component is responsible for the client workstation's enrollment and participation in a NAP protected network and is the real workhorse of the Client NAP architecture.

The NAP EC is tied to the type of access that the client will request and several might be present on a workstation at one time. For instance, a workstation might have separate NAP ECs installed for each of IPSec, 802.1x wired/ wireless access, DHCP, and Terminal Services access. When the workstation needs to participate in one of these connections, the appropriate NAP EC responds by routing the System SoH to the NAP Policy Server to request access and will await the response.

The NAP Enforcement Client will also track the workstation's status in the network and can communicate participation or denial to other requesting components. This is used in cases where overlapping access rights are requested from more than one type of connection simultaneously. In this case, the most restrictive privilege is the winner.

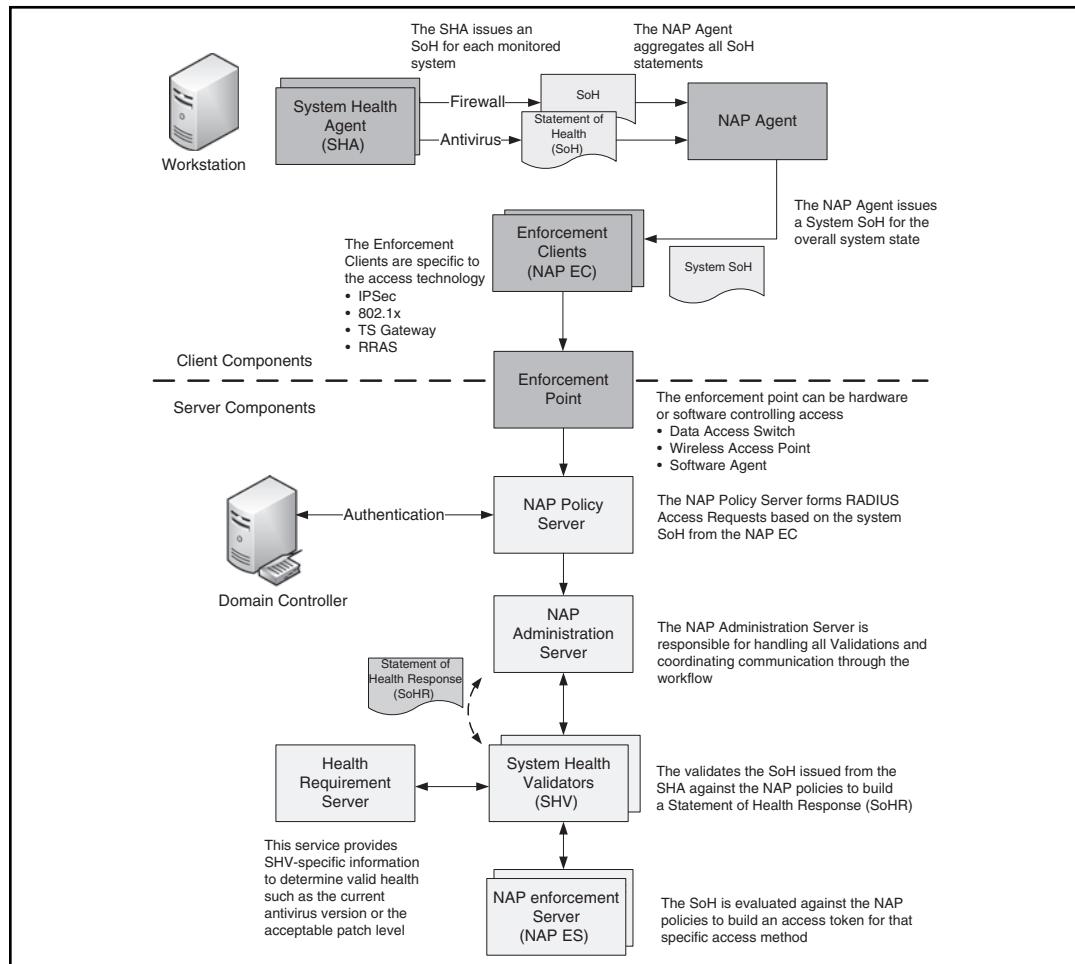
EXAM WARNING

Make sure you understand the difference between the System Health Agent and the NAP Enforcement Client. The SHA is responsible for evaluating the status of the workstation and building the appropriate SoH, whereas the Enforcement client is access method-specific (802.1x, TS Gateway, VPN, and so on).

Network Policy Server

The NAP platform comprises many different parts, each filling a different role in the definition of the network access policy (see Figure 2.5).

Figure 2.5 The NAP Platform



- **NAP Health Policy Server** This component listens on the network for incoming authorization requests from the NAP Enforcement Clients on the workstations. The Health Policy Server will confirm the access request and accept the System SoH relayed in the RADIUS Access-Request message from the NAP EC routing the message to the NAP Administration Server for authorization.
- **NAP Health Registration Authority** This maintains the health certificates for workstations wishing to be authorized through NAP and provides authentication against the domain Certificate Authority.
- **NAP Administration Server** This server is responsible for routing Statement of Health (SoH) messages from workstations to the NAP Administration for Authentication. This server acts as the Authorization step in the full AAA suite, taking the place of the RADIUS service that was in the Windows Server 2003 Internet Authorization Server (IAS).
This server is also responsible for making overall policy decisions based on all SoHR declarations that it receives from the SHVs to build a single access policy for the communication type.
- **System Health Validators (SHV)** For every System Health Agent on the client side, there is a corresponding System Health Validator responsible for the evaluation of the issued SoH against the Network Access Policy.
The SHV generates a Statement of Health Response (SoHR) for each SoH it receives and routes the message to the NAP Administration Server for processing. The SHV can also detect situations for which there is no SoH issued and make access determinations based on this criterion.
- **NAP Enforcement Server (NAP ES)** This is the server component that matches the client-side NAP EC component. The NAP Enforcement Server is responsible for providing the appropriate network access for the access type based on the policy determination from the NAP server.



NOTE

The NAP Enforcement Server can be the same device as the NAP Enforcement Point. In the case of a switch or wireless access point providing 802.1x security, these devices fill both roles. When a client connects to the device, it acts as the Enforcement Point, generating the RADIUS

request that begins the authorization process. Once a determination has been made as to what access is to be granted, the switch or WAP accepts the response—in this case, as a VLAN assignment—to control access.

- **NAP Enforcement Point** This device or service acts as the gatekeeper between the client and server components interfacing with both of them. Table 2.2 lists NAP enforcements points for various access types.

Table 2.2 NAP Enforcement Points

| Access Type | NAP Enforcement Point |
|-------------------------|----------------------------------|
| IPSec Enforcement | Health Registration Authority |
| Wired 802.1x | Hardware Data Switch |
| Wireless 802.1x | Wireless Access Point (WAP) |
| Virtual Private Network | Routing and Remote Access Server |
| DHCP Enforcement | DHCP Server |
| Terminal Server | TS Gateway Server |

- **NAP Requirement Server** This provides additional information to the SHV as to what criteria make a SoH valid for comparison against the policy. A requirement server isn't needed in a case where the requirement is a yes/no question like, "Antivirus must be enabled?" For more complicated evaluations, a separate service might have to provide additional information, "Antivirus must be up to date and have on-access scanning enabled."
- **NAP Remediation Server** In a case where full network access isn't granted because the client workstation has failed to meet the policy requirements for access, the NAP EC may be configured to allow the workstation to reach NAP Remediation Servers. These servers provide resources that can be used by the clients to bring themselves into compliance. This might be a WSUS server, a resource with Antivirus updates, or any other resource determined by the network administrator to be necessary to give the client workstation the resources required to be brought into compliance.

- **Statement of Health Response (SoHR)** For each SoH declaration submitted to the NAP server for evaluation, a SoHR is generated by the System Health Validator comparing the current state of the client against the policy requirements for that health metric. These are used by the NAP ES and Enforcement Point to determine the level of network access granted to the requesting client by the NAP system.

Configuring & Implementing...

Basic Networking Services

A common scenario for NAP is to provide basic networking services to unauthenticated wireless clients while granting full internal network access to domain computers approved to connect through the wireless network. In this case, a separate VLAN is usually created to segment the unauthenticated wireless network traffic from the internal business traffic, controlling access rights, bandwidth utilization, session length, and the types of traffic allowed.

In this case, NAP and RADIUS can validate the workstation's domain membership and assign the correct VLAN to the client, all before it even gets an IP address assigned to it.

Microsoft even includes the Host Credential Authorization Protocol (HCAP) as an NAP option to integrate NAP with Cisco devices that are able to integrate with the Cisco Network Access Control protocols.

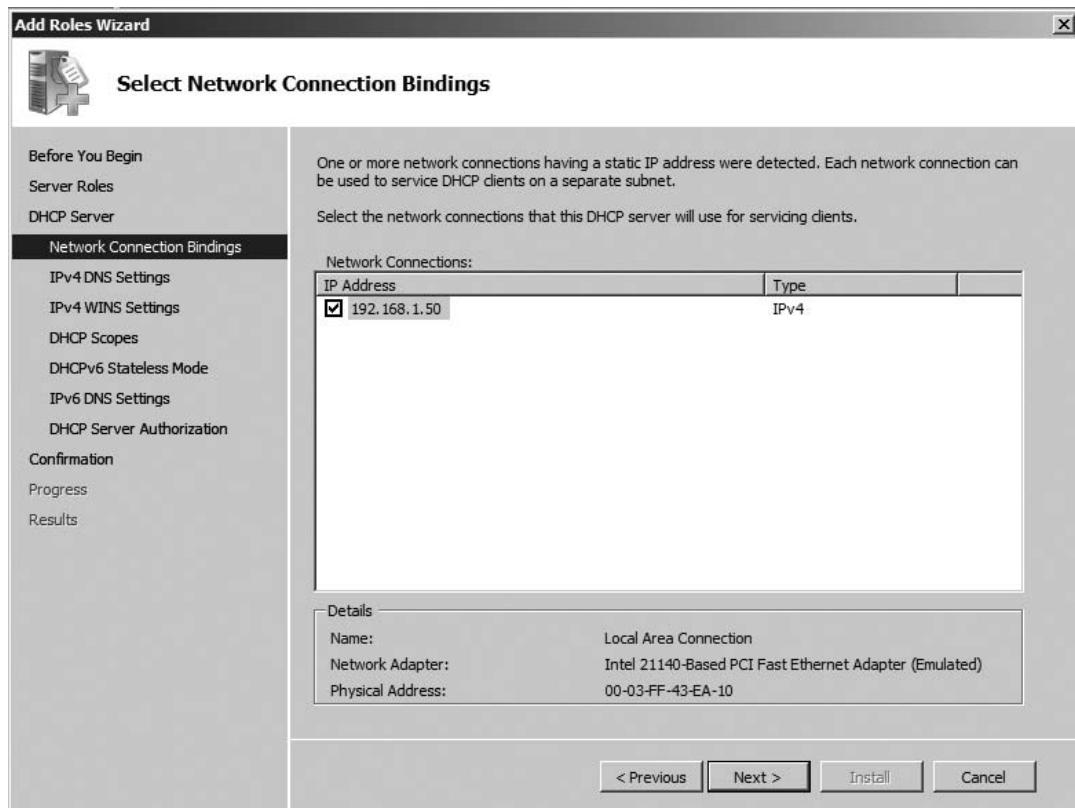
EXERCISE 2.2

CONFIGURING DHCP FOR NAP

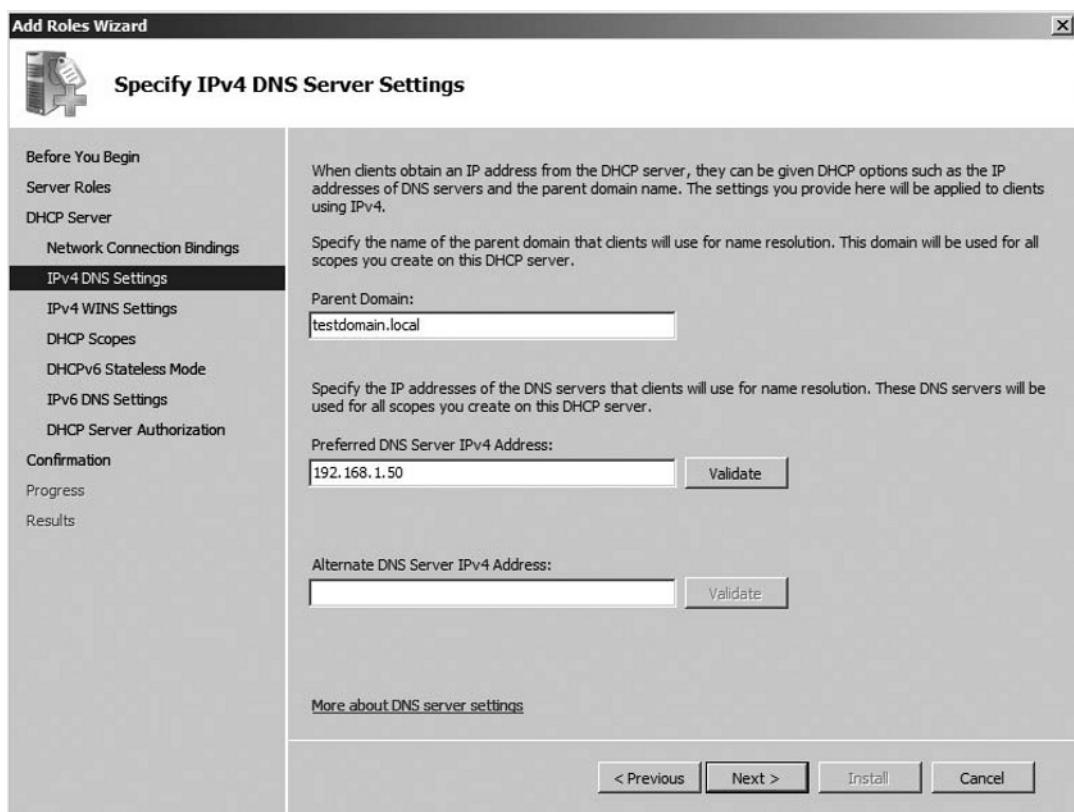
1. To configure DHCP, open Server Manager by choosing **Start | Administrative Tools | Server Manager**.
2. Right-click **Roles** and choose **Add Role**.
3. Check the box for **DHCP Server** and click **Next** twice.

4. On the Select Network Connection Bindings page, select an IPv4 NIC that has already been assigned a static address (see Figure 2.6). Click **Next**.

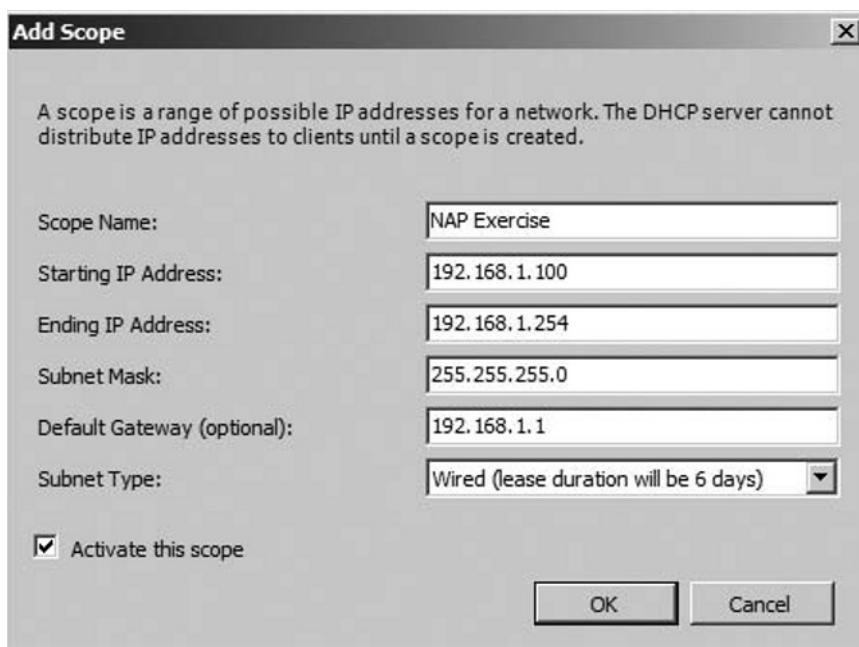
Figure 2.6 Selecting an IPv4 NIC



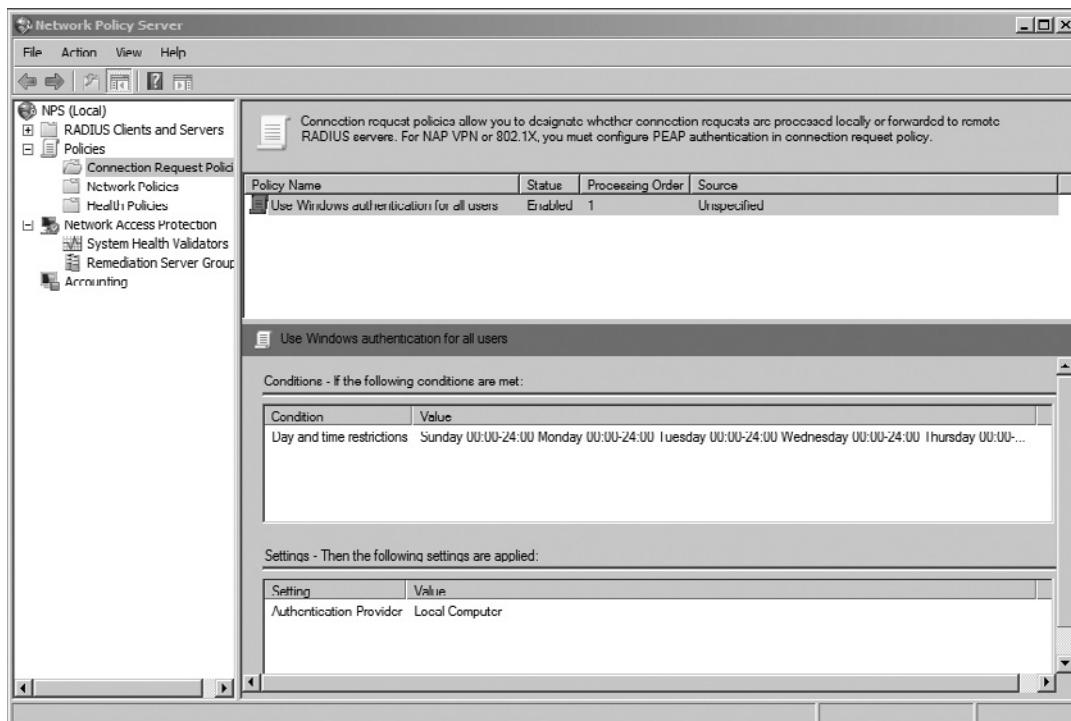
5. On the IPv4 DNS server settings page, ensure that the fully qualified domain name (FQDN) is listed for the domain and that the appropriate AD Integrated DNS servers are listed (see Figure 2.7). Normally, these will be automatically populated from your domain settings.

Figure 2.7 Ensuring That the FQDN Is Listed for a Domain

6. Click the **Validate** button next to each DNS server listed to validate that it is accessible. Click **Next**.
7. On the IPv4 WINS Settings page, specify that WINS is not required for applications on this network. Click **Next**.
8. On the DHCP Scopes Page, click **Add**.
9. On the Add Scope Window (see Figure 2.8):
 - Scope Name: **NAP Exercise**
 - Starting IP Address: **192.168.1.100**
 - Ending IP Address: **192.168.1.254**
 - Subnet Mask: **255.255.255.0**
 - Default Gateway: **192.168.1.1**
10. Ensure that the **Activate This Scope** box is checked and then click **OK**.

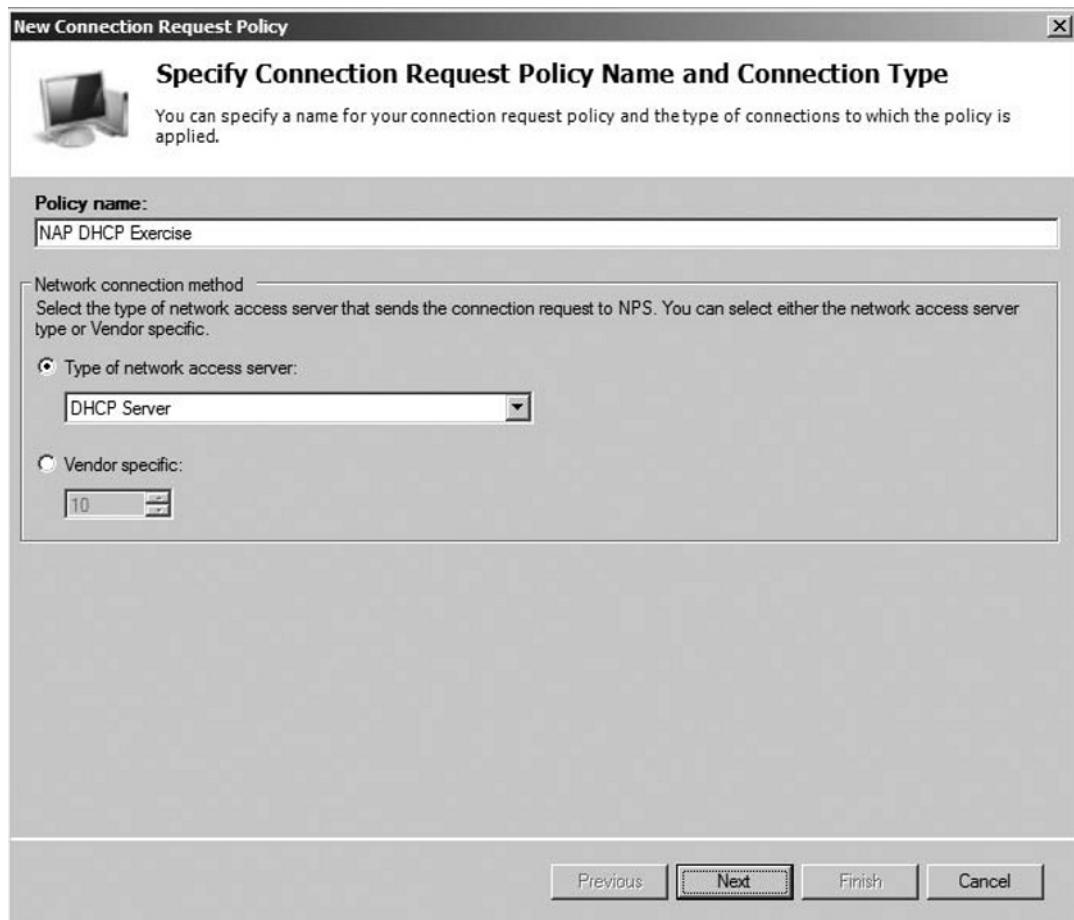
Figure 2.8 The Add Scope Window

11. Click **Next** to confirm the scopes.
12. On the DHCPv6 Stateless Mode, select the radio button to disable this feature. Click **Next**.
13. On the **DHCP Server Authorization** page, ensure that the Domain Administrator credentials have been provided and then click **Next**.
14. Review the server settings and click **Install** to begin the installation.
15. When prompted, click **Close** to complete the installation.
16. To configure NAP, navigate to **Start | Administrative Tools | Network Policy Server** (see Figure 2.9).

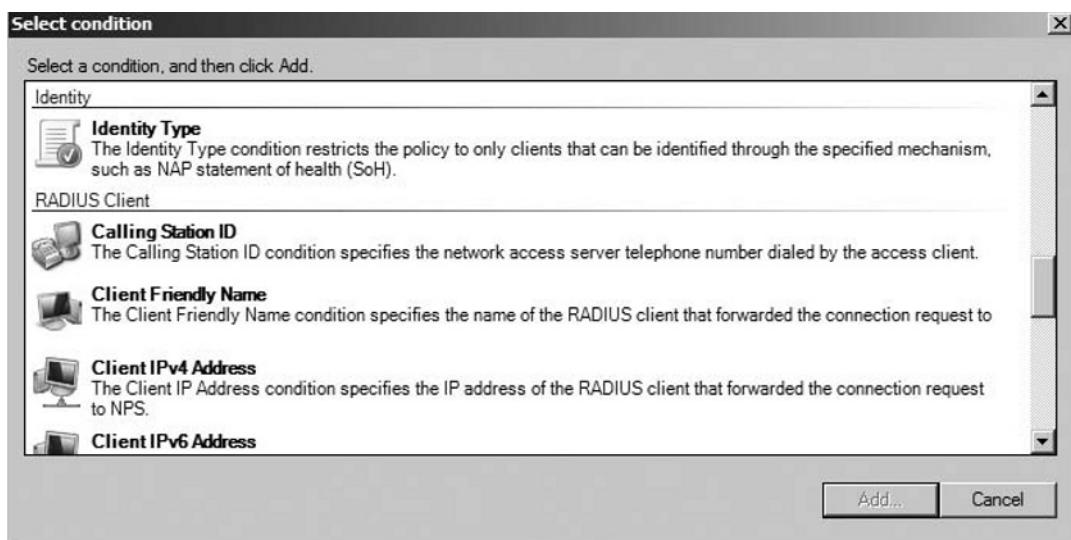
Figure 2.9 The Network Policy Server Page

17. Expand the Policies group. Right-click the **Connection Request Policies** folder and select **New**.
18. Specify the Policy Name as **NAP DHCP Exercise** and select **DHCP Server** as the Type of Network Access Server (see Figure 2.10). Click **Next**.

Figure 2.10 Specifying the Connection Request Policy Name and Connection Type



19. On the **Specify Conditions** page, click **Add**.
20. Choose **Identity Type** (see Figure 2.11) and click **Add**.

Figure 2.11 Selecting Conditions NAP

21. Check the box for **Machine Health check**, click **OK**, and then click **Next**.
22. Ensure that **Authenticate Requests** on this server is selected and click **Next**.
23. Click **Next** to accept the default EAP settings.
24. Click **Next** to accept the RADIUS settings. Then, click **Finish** to create the Connection Request Policy.

Designing a Network for NAP

One of the biggest benefits of NAP is that it allows the network administrator to develop effective network access policies without making dramatic changes to the underlying network structure and without making a significant new investment in hardware. This is certainly true, but a few design principles can be followed that will help get the biggest impact out of a NAP implementation project. NAP logically breaks the network into three segments:

- **Untrusted Segment** This is a segment with minimal permissions and limited access to network resources. In a tightly controlled NAP network, clients that haven't yet authenticated, clients that are not NAP aware, and workstations that do not meet the minimum health requirements are maintained in this segment.

- **Trusted Segment** Once a client has authenticated with the domain and has been certified as meeting the minimum health requirements, it is brought into the trusted segment. Here it is able to fully participate in network communications and access corporate resources.
- **Remediation Segment** The remediation segment contains NAP Remediation Servers and network resources that exist to help bring workstations into compliance. These might be file servers, WSUS servers, antivirus providers, Certificate Authorities, and other third-party application servers that can provide health services to workstations.

It is often helpful to build physical segments or virtual LANs (VLANs) to segment off these types of traffic and to provide additional security through router and switch Access Control Lists (ACLs). This will ensure that your client workstations have the access they need to maintain compliance while protecting your internal network. These VLANs are a logical way to segment a physical network so that access rights and traffic types can be closely controlled. Cisco's Network Access Control (NAC) technology has a wide market deployment, allowing policy-based network admission decisions. A partnership between Microsoft and Cisco has integrated the NPAS policy engine with the Cisco NAC protocols, allowing Cisco switches to act as Policy Enforcement devices with little additional work. This lets companies leverage the hardware and expertise they have built to provide NAP solutions with a much lower cost of adoption.

RADIUS Proxy Server

RADIUS is at the core of NAP technologies, providing the backbone for its communication and enabling it to communicate with both the back-end authentication infrastructure as well as the RADIUS clients that act as enforcement points for the network. When all of these components are on a single network or have no dependencies on external authentication sources, the implementation is fairly straightforward. Unfortunately, complex enterprise networks can conspire against the network administrator putting forth additional business requirements or allowing access to users that are not traditionally part of the domain. In these cases, RADIUS proxy can extend the RADIUS infrastructure beyond the network boundary.

EXAM WARNING

A single NAP solution can work across a number of domains in a single forest, but will require a separate implementation as the environment crosses forest boundaries.

It is not uncommon for a single corporation to have more than one Active Directory forest providing domain services. In this case, each forest will have its own infrastructure supporting AAA and may even have different rules and membership criteria at play. Because of this, it is helpful to connect the corporate RADIUS implementation to the external forest RADIUS using a proxy to forward these requests and routing the response messages back to the RADIUS Clients.

Another common scenario is where certain types of perimeter authentication services are outsourced to a third-party or an ISP that is better able to provide the service. While you might want to maintain a single point of management for your authentication and user identity, it is often overly complicated and expensive to maintain banks of modems and phone lines for dial-up access. Implementing a RADIUS proxy server can allow the ISP to own and operate the dial-up infrastructure while you can maintain the authentication database proxying users' authorization requests into your network.

In all of these scenarios, the key is maintaining the integrity and atomic nature of the Authentication database for appropriate identity management while extending the authorization infrastructure beyond the core network. This reduces the overall maintenance burden since there is only a single location where the user or computer account exists, but the end user is still able to transparently request access to the network.

Remote Access Strategies

Developing a sound remote access strategy is a balancing act weighing the access requirements of the network users against the risk to the environment and the data posed by granting this access. Managing this risk is the key to making appropriate evaluations and driving reasonable compromises that make sense for the business. Remember that the most secure server is the one that is turned off and locked away, but it isn't exactly the most useful or cost effective.

Fortunately, Windows Server 2008 provides a number of remote access methods that can be configured to provide a high level of customer support while at the same time minimizing the risk to the environment. It is important to consider how the end user will access the data and services on the corporate network and the topology over which that access will occur.

Terminal Services for Server 2008

Maintaining the applications that are running on each desktop can be a huge burden for administrators. As such, many organizations choose to run applications on terminal servers rather than install them locally on each workstation. The advantage of doing so is that the application runs on the server, and only video images are sent to the workstations. This makes it much easier for an administrator to maintain the applications.

The terminal services are good for security as well, because applications are much more resistant to user tampering since they do not actually reside on the user's workstations.

In this section, you will learn how to install the Terminal Server Role Service. One of the requirements associated with using the terminal services is that terminal servers must be licensed, and client access licenses are also required. Windows Server 2008 can be configured to act as a Terminal Service Licensing Server, and this chapter shows you how to do it. Finally, you will learn how to establish a client connection to a terminal server.

The primary strength of the terminal services lies in the separation of the running application from the client hardware. The client only needs to be able to run the terminal services client to be able to receive screen updates and route keystrokes and mouse activity to the application server, where all of the heavy lifting is done. The application does not need to route business data across the network in a complicated client/server communication; it can instead merely provide the user interface data to the end user.

Head of the Class...

Where It All Began

The original components of terminal services were created by a company called Citrix Systems, Inc. Headed by a former IBM executive, Citrix became the only company ever to license the Windows NT source code from Microsoft for resale as a separate product. Their popular Windows NT 3.51-derived product was known as WinFrame. Prior to the release of a Windows NT 4.0 related version, Citrix and Microsoft struck a deal in which Microsoft licensed their MultiWin component.

This component lies at the heart of terminal services and enables multiple users to log on locally, as if they were sitting down at the actual server itself. It creates individual sessions for each user and keeps all of their session and application settings separate. The protocol Citrix created to access terminal services was not licensed by Microsoft. It supports a wide range of terminal services clients, load balancing, and application access methods that traditionally have not been supported by Microsoft's remote desktop protocol (RDP). However, with Windows Server 2008, Microsoft is catching up. For the first time, enterprise-level deployments of terminal services are considering going with Microsoft alone and not licensing the additional Citrix services.

Terminal Services can run in two modes:

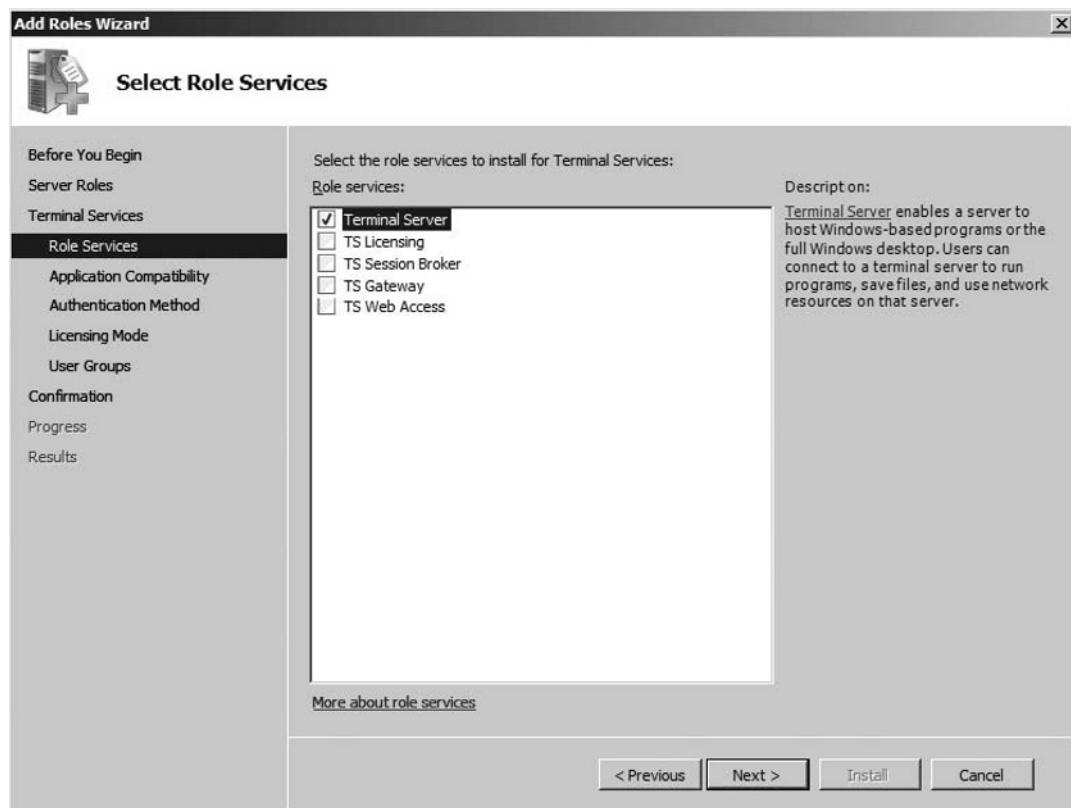
- **Remote Desktop for Administration** This mode is used for remote system administration and is available on all Windows Server Platforms. Additional licensing is not needed to use the Remote Desktop for administration, but only two connections are permitted to connect to the server at any given time.
- **Terminal Services Role** This mode is designed for the sharing of either full remote desktop sessions or remote application windows with end users for production use. The number of connections available for use is dependent upon the server hardware and the number of Terminal Services Client Access Licenses (TS CALs) available.

New to Terminal Services is the ability to provide a single application to the end user through the RDP client rather than a full desktop. This reduces the burden on the network administrator since profiles and security lockdowns for the TS session do not have to be configured. The user experience is also enhanced because the application is indistinguishable from a client-side application to the end user.

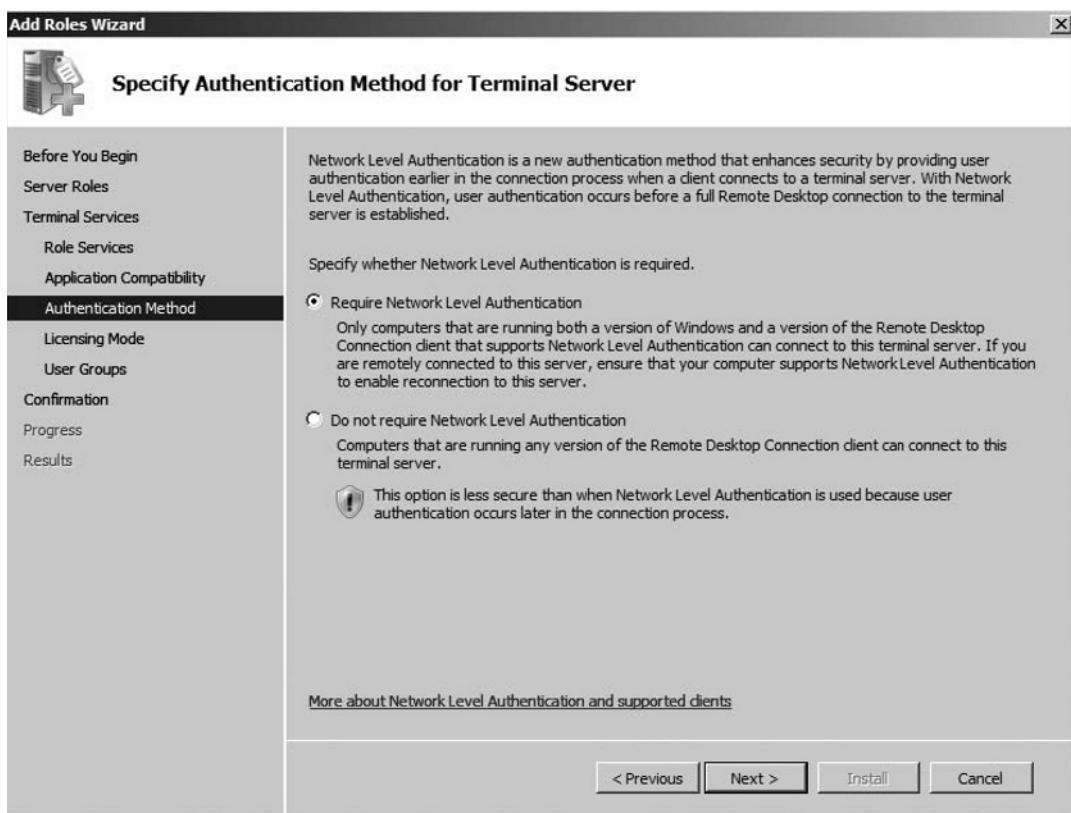
EXERCISE 2.3

CONFIGURING THE TERMINAL SERVICES ROLE

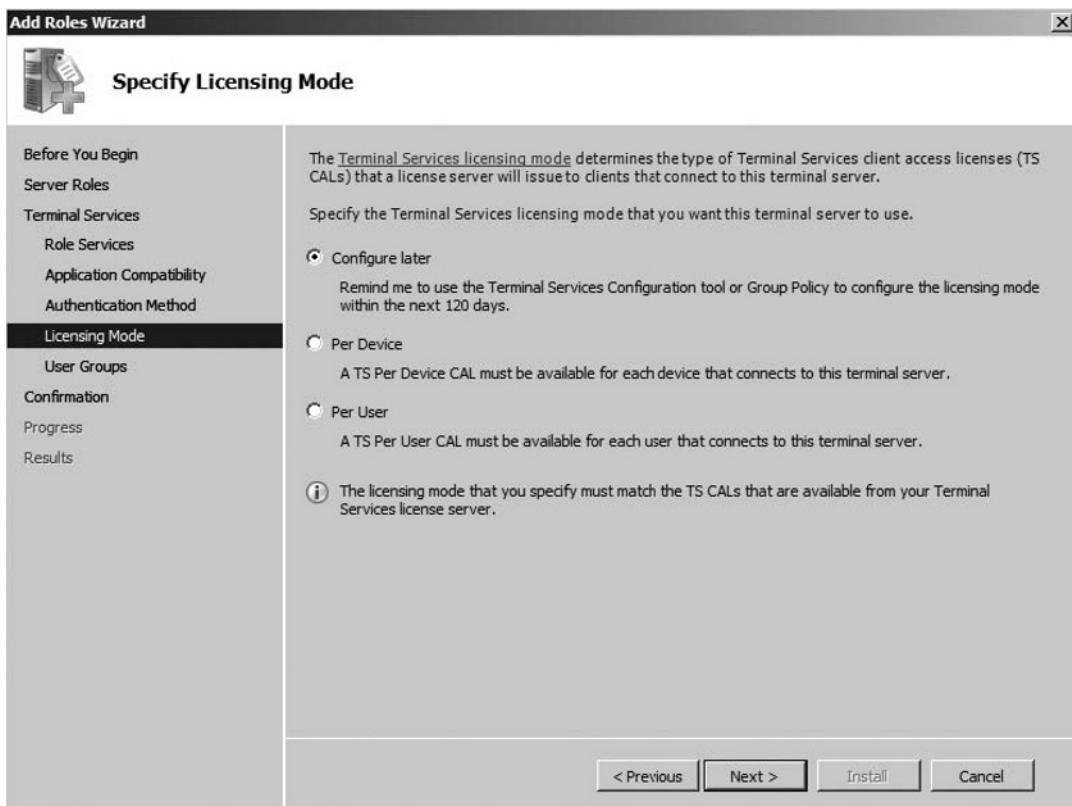
1. Open Server Manager by choosing **Start | Administrative Tools | Server Manager**.
2. Right-click **Roles** and choose **Add Role**.
3. On the information screen, click **Next**.
4. Select Terminal Server (see Figure 2.12) and then click **Next** twice.

Figure 2.12 Selecting the Role Services

5. On the **Authentication Method** page, select the radio button for **Require Network Level Authentication** (see Figure 2.13). Click **Next**.

Figure 2.13 Specifying the Authentication Method

6. On the **Licensing Mode** page, select the radio button for **Configure Later** (see Figure 2.14). This allows Terminal Services to be used for 120 days before a Terminal Services Licensing Server is required. Click **Next**.

Figure 2.14 Specifying the Licensing Mode

Configuring & Implementing...

Licensing Modes

On the licensing mode page, you can choose the following licensing modes:

- **Configure later** This option lets you defer your licensing decision. Microsoft provides a 120-day grace period where temporary licensing can be used. The grace period begins the first time a client connects to the Terminal Server role service. After 120 days, if licensing is not configured, users will not be able to connect to the Terminal Server. If you select this option, each

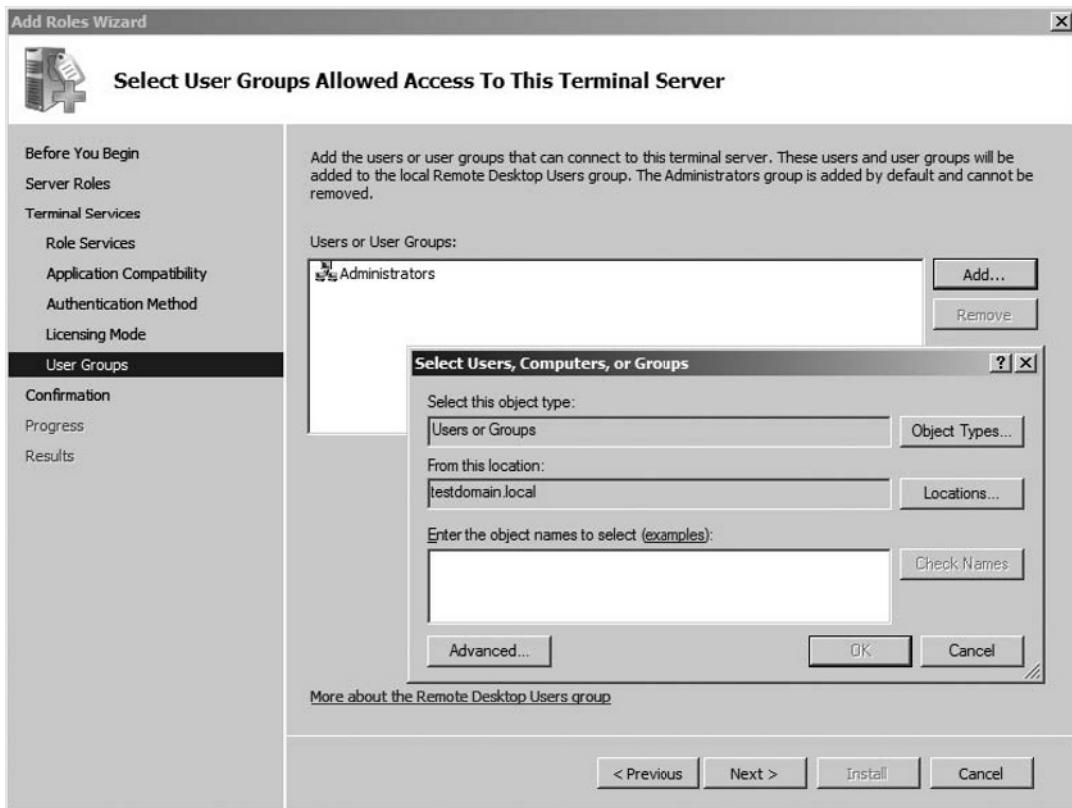
Continued

time you log on to the terminal server a message will appear in the lower right corner reminding you to configure the appropriate licensing mode.

Note: Microsoft allows two administrators to simultaneously connect without requiring Terminal Services access licenses.

- **Per Device** When this option is used, the first time a device (such as a Windows Vista computer) connects to the Terminal Server it will receive a temporary license. The second time it connects, it will receive a permanent license. Under this option, a fixed number of licenses are available, and if no more are available the computer will not be allowed to connect to Terminal Services. See the licensing section in this chapter for information on how to install and configure licensing.
- **Per User** This option assigns licenses to users rather than devices. This type of license provides a user with the right to access a terminal server from any number of client computers or devices. A major difference between Per Device Client Access Licenses (CALs) and Per User CALs is in how they are tracked. Per User CALs are not enforced by the terminal services licensing component, and as a result no user will be rejected because of license unavailability. Under this licensing scheme, the burden is on administrators to ensure they have purchased enough Per User CALs to meet Microsoft's licensing requirements.

7. On the **User Groups** page, click **Add**. On the pop-up, you will be able to add additional users and groups who will be allowed to access terminal sessions (see Figure 2.15). By default, only members of the Administrators are able to connect to terminal services. Click **OK**, and then **Next**.

Figure 2.15 Selecting User Groups

8. Validate that the settings are correct on the Information screen.
Click **Install**.
9. Click **Close** to allow the server to reboot to complete the installation process.

Configuring & Implementing...

Proper Terminal Server Planning

The Terminal Server role service can use up considerable resources. When a user establishes a terminal server session, it's very similar to a workstation

Continued

being created on the terminal server for them to use. Imagine what happens when a server has 20 or more of these workstations all running on it at the same time. If the server hardware and configuration is not adequately sized to the number of users, performance can degrade rapidly. The number one mistake made when installing terminal servers is failure to accurately estimate the amount of resources that will be needed to adequately serve users.

Another important consideration is security. Typically, users connect to servers as remote users. However, when users log on to a terminal server, they log on as a local user. There are substantial differences in user rights between local and remote users that administrators can easily overlook when configuring terminal services. Locking down the security on a terminal server is more art than science, and you should do everything possible to learn the best practices available from Microsoft regarding it.

New Roles

While Terminal Services has been available to the Windows community for a number of years, it has largely operated in isolation, making true enterprise deployment of terminal-enabled applications difficult. Providing highly available yet secure solutions was challenging and not natively built into the product forcing some network administrators to move to other third-party solutions.

Head of the Class...

Adoption of Citrix Technology

Before Windows Server 2008, organizations would usually implement the third-party product Citrix Presentation Server when application needs required server farms, gateway services, load balancing, or Web access. This required licensing in addition to the Terminal Services Client Access Licenses (TS CALs) and a high level of expertise to configure.

The inclusion of these services in the Windows Server product makes adoption of the technology much easier and more accessible to network administrators. This also allows applications already configured in earlier versions of terminal services to take advantage of these new features and support a wider community of users.

In addition to the familiar Terminal Services and TS Licensing, Windows Server 2008 introduces several new server roles to bring enterprise functionality.

- **Terminal Services Session Broker** One of the major downfalls of previous versions of terminal services was the standalone nature of individual terminal servers. As applications became available across an organization through Terminal Services, additional standalone servers would have to be configured.

The TS Session Broker lets servers be grouped into application farms that are intimately aware of node status and load so that client session requests can be directed to the node that will provide the best performance. This provides better availability for the application since dead or oversubscribed nodes are not sent additional connections. Scalability is also improved because this provides the ability to grow the environment as needed rather than in a step-wise deployment.

- **Terminal Services Gateway** Using Terminal Services on an internal network is relatively simple: users are usually already authenticated to the network, there isn't a need for a high level of encryption, and all of the clients can connect directly to the terminal servers. Making terminal sessions available to remote users introduces security concerns for the connection and can be complicated by restrictions on the client's network.

The Terminal Services Gateway acts as a single point of contact, handling these inbound connection requests. Rather than requiring that you open the ports associated with the Remote Desktop Protocol (RDP) to the outside world, the TS Gateway listens on the SSL port (TCP/ 443) commonly used for secure Web sites. The gateway then forwards the request to the Terminal Server. This means that the surface area of attack is reduced on the server network and that complicated VPNs and firewall rules don't need to be configured for client access.

EXAM WARNING

The TS gateway requires that IIS be installed, as well as RPC over HTTP. These are to allow external Web services to be exposed for the handling of inbound connections.

The TS Gateway can also act as an Enforcement Point and an Enforcement Server in a NAP configuration, requiring that connecting workstations meet basic criteria before they are allowed to connect to the

Terminal Servers. This gives the network administrator the best of both worlds—client connections are more easily able to connect to the Terminal Services infrastructure, while at the same time security is improved by securing the connection, reducing the surface area of attack, and requiring that the connecting machines meet base criteria.

- **Terminal Services Web Access** In some circumstances, it is not practical to install Terminal Service client software on remote workstations either because of network security constraints on the computers or because the access is for one-time use. Terminal Services Web Access allows any client with a Web browser to connect to the terminal server to use the desktop or TS-enabled applications.

Developing a Terminal Services Remote Access Strategy

One of the prime decisions that must be made when developing a Terminal Services implementation is how these services will be made available to the users. Usually, all Terminal Services sessions will be established through the Terminal Services Gateway because this acts as a single point of management where NAP rules can be applied and more comprehensive auditing done. It might seem easier to allow users to connect directly to terminal servers, but it is much easier to implement a gateway before the application is in production and considered part of the IT environment.

It is also important to evaluate the business's tolerance for system failure and the service level that is required of the Terminal Services environment. This will help determine the number of servers that should be deployed and whether more advanced features like Session Broker are required (see Figure 2.16).

Figure 2.16 Evaluating Required Service Levels in Terminal Services Environments

| Requirement | Technology | | |
|----------------------------|----------------|---------------------------|------------|
| | Session Broker | Terminal Services Gateway | Web Access |
| High Availability | x | | |
| NAP Policy | | x | |
| Access through a Firewall | | x | x |
| Uncontrolled RDP Client | | | x |
| Clients not Domain Members | | x | x |

NOTE

In practice, it is often helpful to deploy Terminal Services farms of three or more individual nodes. This allows one node to be down for maintenance (or due to trouble) while the other two servers maintain the production load. You might be tempted to only deploy two servers, but for mission-critical applications, it is usually better to avoid reducing your farm to a single point of failure every time you want to upgrade an individual server.

The Corporate Desktop

Traditionally, Terminal Services has worked as an extension of the Remote Desktop concept, where a full desktop is deployed to the client. In this mode, the end user is able to use the machine as though it were a physical workstation. This enabled a special class of workstation device called thin clients to act as low-cost workstations, with only enough horsepower to run the RDP client, allowing the terminal server to do all of the real computational work. These devices are easily interchangeable and often have no moving parts; however, they *are* losing market share as workstation prices drop.

Configuring the corporate desktop is simple and requires almost no configuration to simply establish a connection. In practice, it requires significant planning and testing to be viable. Because a full desktop is presented to the end user in a shared environment, changes made by one user have the potential to impact the entire terminal services community using this server. This is especially true of users with administrator rights who have the ability to add programs and change the system configuration.

When deploying the corporate desktop as an enterprise solution, it is important to make extensive use of Group Policy, folder redirection, and security settings to control access rights and mitigate the risk introduced by the shared platform. Especially useful are roaming profiles and terminal services profiles that allow users to receive a consistent user experience when connecting to a farm of Terminal Services servers. Without these, changes made when attached to one server would appear to be missing if the user attached to a different server in the farm on the next connection.

New & Noteworthy...

Windows Vista Experience

Providing a server desktop to end users can be confusing because they generally don't have any experience with the server operating system and can be confused by its restrictions. Windows Server 2008 offers a new feature to help bridge this gap. The Windows Vista Experience feature can present a Vista-like desktop to users, giving them the desktop experience they expect from the server-class platform.

RemoteApp Programs

With Windows Server 2008, Microsoft has introduced the RemoteApp feature into Terminal Services. This allows a single application to be shared as a Terminal application with end users. Rather than having access to the entire desktop, only the application window is shared with the end user. This means that the Terminal experience is seamless and the user may not even know they are using a terminal application to get work done.

Deploying applications this way has long been only available to third-party applications like Citrix presentation server and other add-ons to Terminal Services. Now, this functionality can be deployed without the overhead and additional configuration needed to configure these services. This means that RemoteApps can be made available to end users without having to configure the extensive security and group policy settings required by the corporate desktop.

In order to connect to a program shared as a RemoteApp, you must use version 6.1 of the RDP client. This is available with Windows Server 2008, Windows Vista SP1, and Windows XP SP3.

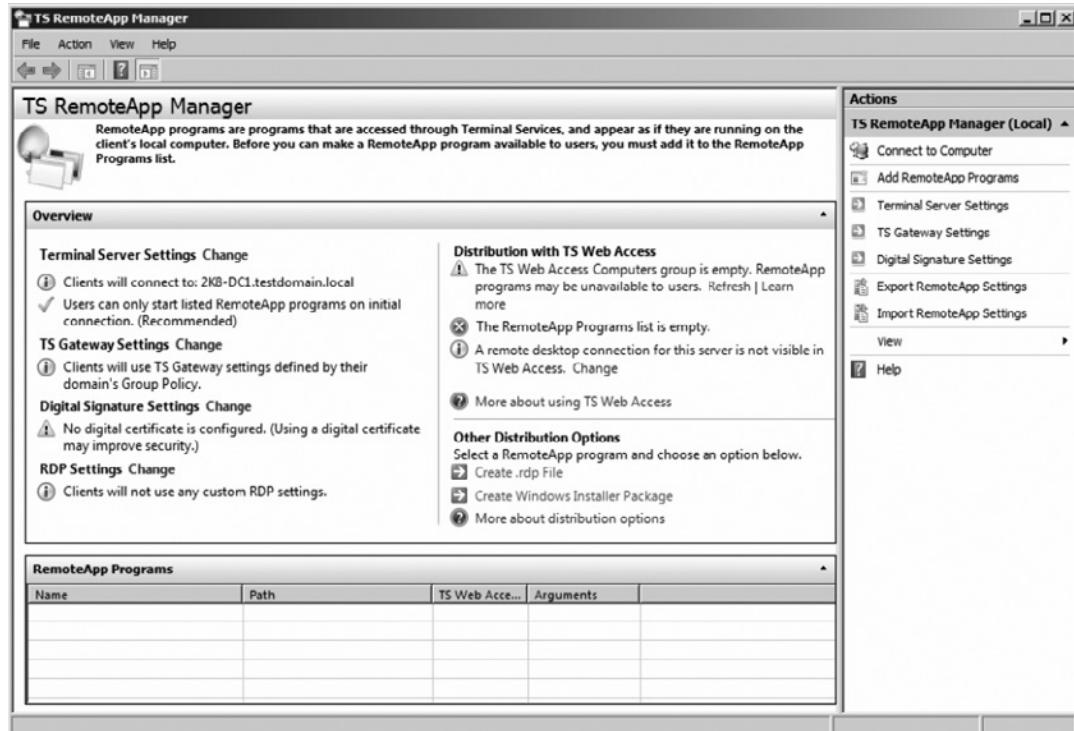
EXERCISE 2.4

CONFIGURING A REMOTEAPP PROGRAM

In this exercise, we will configure the calculator application to be available through Terminal Services as a RemoteApp.

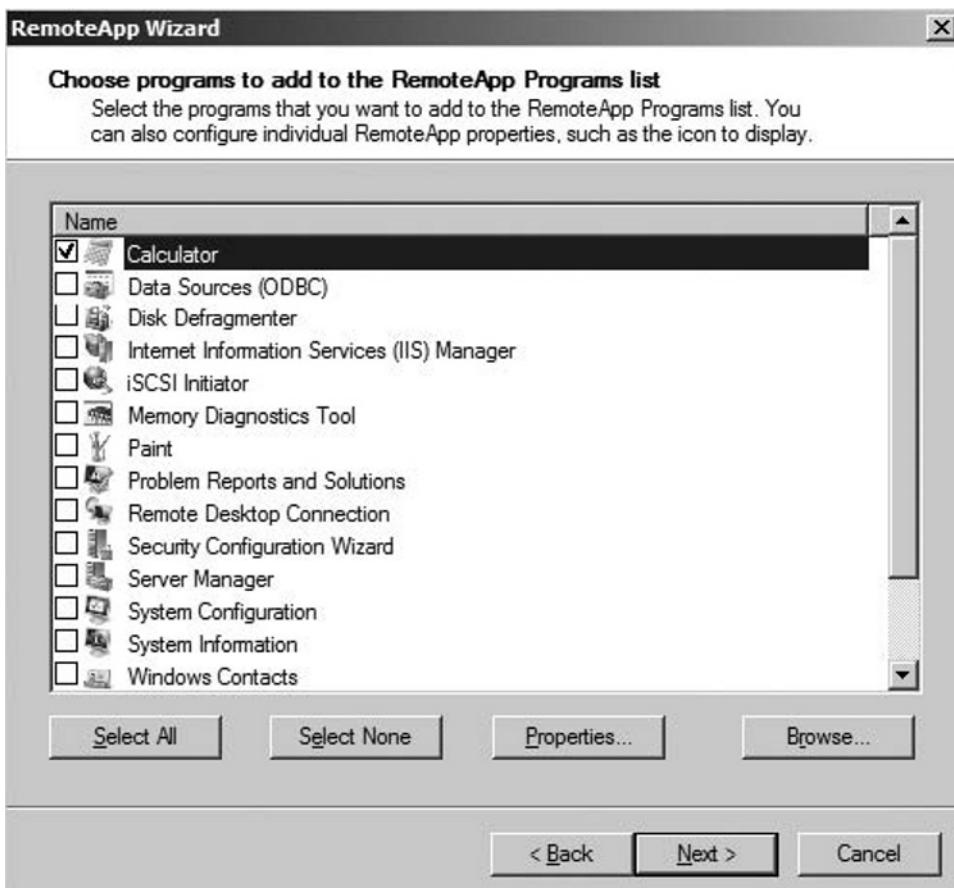
1. To create the RemoteApp program, navigate to **Start | Administrative Tools | Terminal Services**.
2. Open the **TS RemoteApp Manager** (see Figure 2.17).

Figure 2.17 TS RemoteApp Manager



3. In the **Actions** Pane, click **Add RemoteApp Programs** to start the RemoteApp Wizard.
4. Click **Next** to begin the wizard.
5. The wizard will display installed applications that can be shared as RemoteApps. In this case, choose **Calculator** (see Figure 2.18) and click **Next**.

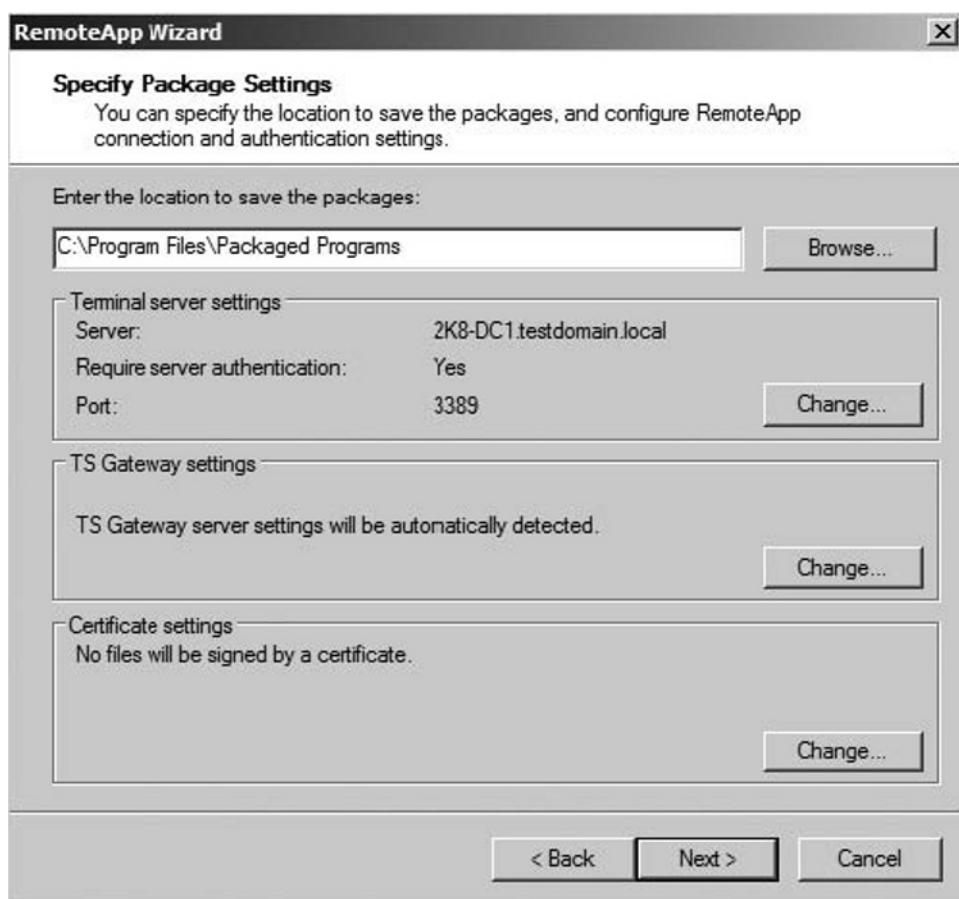
Figure 2.18 Choosing Programs to Add to RemoteApp



6. Review the Settings for the application and click **Finish**.

Now, we'll show you how to build an .rdp file for application deployment.

1. In the RemoteApp Programs Pane, right-click the **Calculator** app you just created. Choose **Create .rdp file**.
2. The RemoteApp Wizard will start (see Figure 2.19). Click **Next**.

Figure 2.19 The RemoteApp Wizard

3. Click **Next** to accept the default configuration.
4. Review the application settings and click **Finish** to create the .rdp file.

To test the new RemoteApp, follow these steps:

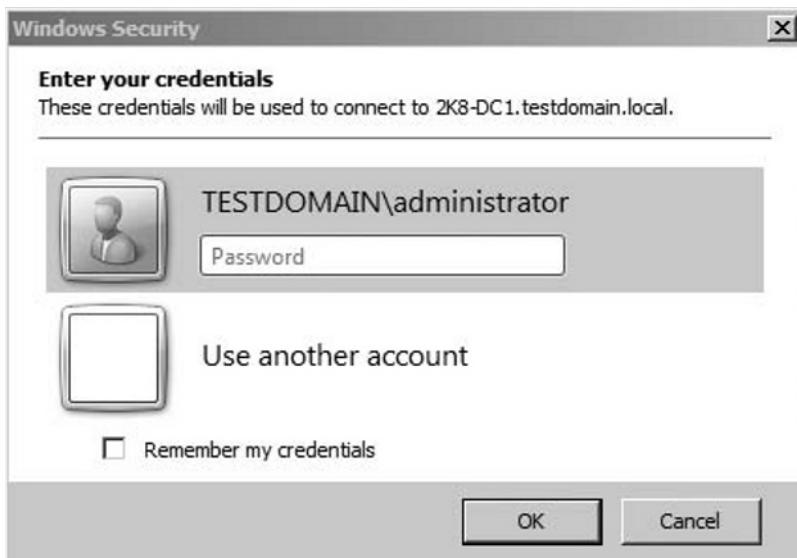
1. To test the new RemoteApp, double-click the .rdp file you just created. (By default, this is located at C:\Program Files\Packaged Programs.)
2. If you get a Security Warning, click **Connect** to accept the connection (see Figure 2.20).

Figure 2.20 RemoteApp Program Security Warning



3. Provide valid domain credentials with rights to connect to Terminal Services sessions (see Figure 2.21).

Figure 2.21 Entering Your Credentials



4. The Calculator application will open on the desktop as a RemoteApp and should be indistinguishable from a traditional application. Close the application as you normally would.
-

Terminal Services Licensing

In addition to the normal Windows Client Access Licenses (CALs) that users and devices need to access Windows Server 2008, additional Terminal Services Client Access Licenses (TS CALs) are required to connect to Terminal sessions. These licenses must be separately purchased and are not included with the operating system, though they are not needed for the two Remote Desktop connections allowed on each server for administration.

The Terminal Services Licensing role is responsible for the tracking and maintenance of the TS CALs, acting as a license database and assigning them to users and devices requesting access to Terminal Services. When a client makes a connection request to begin a terminal session, the server will locate the appropriate TS Licensing server to check that the user or device has a valid TS CAL assigned to it. If one has not been issued, a request will be sent to the licensing server to issue a TS CAL before the session will be granted. In cases where a TS Licensing server has not yet been deployed in the environment, per-device connections will be permitted during the grace period. This grace period will last until a license server becomes available or the grace period runs out.



NOTE

On Windows Server 2008 and 2003, the grace period for Terminal Service licensing is 120 days from the time the first terminal connection is made. This period is only 90 days on Windows Server 2000.

Installing a Terminal Service Licensing Server

The TS Licensing role service has three primary installation methods:

- If you are installing the Terminal Server and TS Licensing role services on the same server, you can install them at the same time.
- You can install the TS Licensing role service on an existing Terminal Server.

- You can install the TS Licensing role service on a separate server.

Microsoft will most likely test you on the separate installation steps, so we cover both ways of accomplishing this in the following. First, we will install the TS Licensing role service on a server that the Terminal Server role service is already installed on. Next, we will install the role service on a separate server.

Installing the TS Licensing Role Service on an Existing Terminal Server

Perform the following steps to install the TS Licensing role service:

1. Open Server Manager by choosing **Start | Server Manager**.
2. Navigate to the **Terminal Services** role by either:
 - Scrolling down in the right pane to the **Roles Summary** section and clicking **Terminal Services**, or...
 - In the left pane, expanding the **Roles** node and clicking **Terminal Services**.
3. In the right pane, click **Add Role Services**.
4. The Add Role Services wizard appears. On the Select Role Services page, select **TS Licensing** and click **Next**.
5. On the **Configure Discovery Scope for TS Licensing** wizard page, select the appropriate licensing option, such as:
 - **This workgroup** If the server you are installing the TS Licensing role service on is not a domain member, this option will be enabled. When used, terminal servers in the same workgroup can locate the license server without any additional configuration.
 - **This domain** This is the default setting for TS Licensing role service servers that are domain members. If the server is also a domain controller, terminal servers that are members of the same domain can locate the license server without any additional configuration. If the server is not a domain controller, it must be published in Active Directory (AD) for terminal servers in its domain to locate it. See the “Publishing a Terminal Services Licensing Server Using TS Licensing Manager” section in this chapter for more information. To select this option, you must be logged on as a domain administrator from the domain in which the server is a member.

- **The forest** This is the recommended setting for TS Licensing role service servers that are domain members. When used, terminal servers that are members of any domain in the forest can locate the license server without any additional configuration. To select this option, you must be logged on as an enterprise administrator from the forest in which the server is a member.
6. Select a new location for the TS Licensing database by clicking **Browse...** or accept the default path, and then click **Next**. The database location must be a local folder on the server on which TS Licensing is being installed.
 7. On the **Confirm Installation Selections** wizard page, review the information you provided and click **Install**.
 8. The Installation Progress screen will provide information about the installation as it progresses. Review the information presented on the Installation Results wizard page, then click **Close**.

Installing the TS Licensing Role Service on a Separate Server

Perform the following steps to install the TS Licensing role service:

1. Open Server Manager by choosing **Start | Server Manager**.
2. In the right pane, scroll down to the **Roles Summary** section and click **Add Roles**.
3. If the **Before You Begin** page of the Add Roles Wizard appears, click **Next**. If this screen does not appear, proceed to the next step.
4. On the **Select Server Roles** wizard page, select **Terminal Services** and then click **Next**.
5. Read the introductory information on the Terminal Services wizard page, and then click **Next**.
6. On the **Select Role Services** wizard page, select **TS Licensing** and click **Next**.
7. On the **Configure Discovery Scope for TS Licensing** wizard page, select the appropriate licensing option:
 - **This workgroup** If the server you are installing the TS Licensing role service on is not a domain member, this option will be enabled. When used, terminal servers in the same workgroup can locate the license server without any additional configuration.

- **This domain** This is the default setting for TS Licensing role service servers that are domain members. If the server is also a domain controller, terminal servers that are members of the same domain can locate the license server without any additional configuration. If the server is not a domain controller, the server must be published in AD for terminal servers in its domain to locate it. See the “Publishing a Terminal Services Licensing Server Using TS Licensing Manager” section in this chapter for more information. To select this option, you must be logged on as a domain administrator from the domain in which the server is a member.
- **The forest** This is the recommended setting for TS Licensing role service servers that are domain members. When used, terminal servers that are members of any domain in the forest can locate the license server without any additional configuration. To select this option, you must be logged on as an enterprise administrator from the forest in which the server is a member.



TEST DAY TIP

Microsoft often uses default settings that are different than their recommended settings. The settings *This domain* and *This forest* are good examples. It's important for you to know not only what Microsoft recommends, but also what the default settings are when they differ.

8. Select a new location for the TS Licensing database by clicking **Browse...** or accept the default path, and click **Next**. The database location must be a local folder on the server on which TS Licensing is being installed.
9. On the **Confirm Installation Selections** wizard page, review the information you provided and click **Install**.
10. The Installation Progress screen will provide information about the installation as it progresses. Review the information presented on the Installation Results wizard page, and then click **Close**.

Activating a Terminal Service Licensing Server

After installing the TS Licensing role service, it must be activated. Microsoft provides a grace period of 90 days during which the license server can issue temporary TS

CALs, but you should activate the server as soon as possible after installation. Three methods of activation can be used for the TS Licensing Manager utility:

- **Automatic connection (recommended)** This method uses TS Licensing Manager to connect directly to the Microsoft Clearinghouse using TCP port 443. The connection occurs from the computer running TS Licensing Manager, which can be a workstation or server. Microsoft also refers to this method as *Internet (automatic)*.
- **Web Browser** If the computer running TS Licensing Manager cannot access the Microsoft Clearinghouse via the Internet, you can complete the process through a standard Web browser from another computer.
- **Telephone** If you cannot use either of the previous methods, the process can also be completed by phone.

Let's examine how to use each method.

Activating a Terminal Service Licensing Server Using the Automatic Connection Method

Follow these steps to use the Automatic connection (recommended) installation method:

1. Open the TS Licensing Manager utility by choosing **Start | Administrative Tools | Terminal Services | TS Licensing Manager**.
2. When the utility opens, it will bring up the Finding Licensing Servers window, and search for all servers running the TS Licensing role service that it can find. In the right pane, right-click the server you want to activate and select **Activate Server** from the context menu.
3. Read the Welcome to the Activate Server Wizard page of the Activate Server Wizard, and then click **Next**.
4. On the **Connection Method** wizard page, select **Automatic connection (recommended)** in the drop-down box, read the information presented, and then click **Next**.
5. A brief dialog window appears while the wizard connects to the Internet and locates the Microsoft Clearinghouse. On the **Company Information** wizard page, enter your information into the **First Name, Last Name**, **Company**, and **Region or Country** fields. Click **Next**.

6. A second **Company Information** wizard page appears. The information asked for by this page is optional. The fields provided are **E-mail**, **Organizational unit**, **Company address**, **City**, **State/province**, and **Postal code**. Once you have filled in the desired fields, click **Next**.
7. A brief **Activating the license server** dialog appears, after which your license server is activated.
8. On the **Completing the Activate Server Wizard** page, do one of the following:
 - Select **Start Install Licenses Wizard now** to proceed to installing TS CALs onto your license server. Click **Next** and follow the instructions.
 - Deselect **Start Install Licenses Wizard now**, and click **Finish**.
(Note: the button text changes between *Next* and *Finish* based on whether **Start Install Licenses Wizard now** is selected.)

EXERCISE 2.5

INSTALLING AND ACTIVATING TS LICENSING ROLE SERVICE

In this exercise, we will install the TS Licensing role service on the same server you installed the Terminal Server role service on in Exercise 2.3. So, you should complete Exercise 2.3 before performing this exercise. Since we will be using the Automatic connection (recommended) method, your server will need access to the Internet. Perform the following steps to install and activate the TS Licensing role service:

- 1 Open Server Manager by choosing **Start | Server Manager**.
2. Navigate to the Terminal Services role by either:
 - Scrolling down in the right pane to the Roles Summary section and clicking **Terminal Services**, or...
 - In the left pane, expanding the **Roles** node and clicking **Terminal Services**.
3. In the right pane, click **Add Role Services**.
4. The Add Role Services wizard appears. On the **Select Role Services** page, choose **TS Licensing** and click **Next**.

5. On the Configure Discovery Scope for TS Licensing wizard page, select the appropriate licensing option: **This workgroup**, **This domain**, or **The forest**.
 6. Select a new location for the TS Licensing database by clicking **Browse** or accepting the default path, and then click **Next**. The database location must be a local folder on the computer on which TS Licensing is being installed.
 7. On the **Confirm Installation Selections** wizard page, review the information you provided and click **Install**.
 8. The Installation Progress screen will provide information about the installation as it progresses. Review the information presented on the **Installation Results** wizard page, then click **Close**.
 9. Open the TS Licensing Manager utility by choosing **Start | Administrative Tools | Terminal Services | TS Licensing Manager**.
 10. In the right pane, right-click the server you want to activate and select **Activate Server** from the context menu.
 11. Read the Welcome to the Activate Server Wizard page of the Activate Server Wizard, and click **Next**.
 12. On the Connection Method wizard page, select **Automatic connection (recommended)** in the drop-down box, read the information presented, and click **Next**.
 13. On the Company Information wizard page, enter your information into the **First Name**, **Last Name**, **Company**, and **Region or Country** fields.
 14. Click **Next**.
 15. On the second **Company Information** wizard page, optionally, enter information in the **E-mail**, **Organizational unit**, **Company address**, **City**, **State/province**, and **Postal code** fields. Once you have filled in the desired fields, click **Next**.
 16. A brief **Activating the license server** dialog appears, after which your license server is activated. On the **Completing the Activate Server Wizard** page, deselect **Start Install Licenses Wizard now**, and then click **Finish**.
-

Activating a Terminal Service Licensing Server Using the Web Browser Method

The following steps can be used to activate the TS Licensing role service via your Web browser:

1. Open the TS Licensing Manager utility by choosing **Start | Administrative Tools | Terminal Services | TS Licensing Manager**.
2. When the utility opens, it will bring up the Finding Licensing Servers window and search for all servers running the TS Licensing role service it can find. In the right pane, right-click the server you want to activate and select **Activate Server** from the context menu.
3. Read the Welcome to the Activate Server Wizard page of the Activate Server Wizard, and then click **Next**.
4. On the Connection Method wizard page, select **Web Browser** in the drop-down box, read the information presented, and then click **Next**.
5. The License Server Activation wizard page appears, which provides the Terminal Server Licensing Web site URL, as well as the Product ID you will need to enter. Click the hyperlink to visit the Web site or open a Web browser and type in the URL (<https://activate.microsoft.com>).
6. On the first page of the Terminal Server Licensing Web site, select **Activate a license server** and click **Next**.
7. Enter your **Product ID** as well as information for the following required fields: **Last/Surname**, **First/Given Name**, **Company**, and **Country/Region**. You can also choose to fill in several optional fields, such as **Organizational Unit**, **eMail Address**, **Phone Number**, **Company Address**, **City, State/Province**, and **Postal Code**.
8. Click **Next**.
9. Review and verify the information you provided, and then click **Next**.
10. Write down the license server ID that is displayed and/or print the Web page.
11. Switch back to the **License Server Activation** page in TS Licensing Manager.
12. Enter the license server ID you received, and then click **Next**. A brief **Activating the license server** dialog appears, after which your license server is activated.

13. On the **Completing the Activate Server Wizard** page, do one of the following:
 - Select **Start Install Licenses Wizard now** to proceed to installing TS CALs on your license server. Click **Next** and follow the instructions. Installing TS CALs is covered in the “Managing Terminal Services Client Access Licenses (TS CALs)” section of this chapter.
 - Deselect **Start Install Licenses Wizard now**, and click **Finish**.
(Note: the button text changes between *Next* and *Finish* based on whether the **Start Install Licenses Wizard now** is selected.)

Activating a Terminal Service Licensing Server Using the Telephone Method

The following steps can be used to activate the TS Licensing role service via the telephone:

1. Open the TS Licensing Manager utility by choosing **Start | Administrative Tools | Terminal Services | TS Licensing Manager**.
2. When the utility opens, it will bring up the Finding Licensing Servers window, and search for all servers running the TS Licensing role service it can find. In the right pane, right-click the server you want to activate and select **Activate Server** from the context menu.
3. Read the Welcome to the Activate Server Wizard page of the Activate Server Wizard, and click **Next**.
4. On the **Connection Method** wizard page, select **Telephone** in the drop-down box, read the information presented, and then click **Next**.
5. The Country or Region Selection wizard page appears. Click your country or region in the **Country or Region:** selection box, and then click **Next**.
6. The License Server Activation wizard page appears, which shows the telephone number to call, as well as the Product ID. Call Microsoft at the number given and provide all requested information. The Microsoft representative you speak to will process your request and give you your license server ID.
7. Switch back to the **License Server Activation** wizard page in TS Licensing Manager.

8. Enter the license server ID you received from Microsoft, and click **Next**. A brief **Activating the license server** dialog appears, after which your license server is activated.
9. On the **Completing the Activate Server Wizard** page, do one of the following:
 - Select **Start Install Licenses Wizard now** to begin installing TS CALs onto your license server. Click **Next** and follow the instructions. Installing TS CALs is covered in the “Managing Terminal Services Client Access Licenses (TS CALs)” section of this chapter.
 - Deselect **Start Install Licenses Wizard now**, and click **Finish**. (Note: the button text changes between *Next* and *Finish* based on whether the **Start Install Licenses Wizard now** is selected.)

Establishing Connectivity between Terminal Server and Terminal Services Licensing Server

As mentioned in the “Installing a Terminal Service Licensing Server” section of this chapter, the way you deploy a TS Licensing server relates directly to how a Terminal Server finds and uses it. Three discovery scope configurations can be specified during the installation of the TS Licensing role service: the Workgroup Discovery Scope (*This workgroup*), the Domain Discovery Scope (*This domain*), and the Forest Discovery Scope (*The forest*). You must also decide which server will host the role. The TS Licensing role service can be installed on a domain controller, a server running the Terminal Server role service, or a separate server that is a workgroup or domain member.

TEST DAY TIP

 Microsoft often changes the name of key items between releases, and then tests you on it. Be on the lookout for these types of exam tactics. For example, Forest Discovery Scope in Windows Server 2008 TS Licensing was referred to as the *Enterprise Scope* in Windows Server 2003. It's especially important to try to learn new terms as Microsoft adopts them. They expect their certified professionals to be able to accurately represent their products' features in the marketplace.

If the server you are installing the TS Licensing role service on is not a domain member, the *This Workgroup* option will be enabled. When used, terminal servers in the same workgroup can locate the license server without any additional configuration. If you later join the server to a domain, the discovery scope will be automatically changed from *This Workgroup* to *This Domain*.

The default setting for a TS Licensing role service server that is a domain member is *This domain*. Although the wizard defaults to this option, Microsoft recommends using Forest Discovery Scope as the setting for all TS Licensing role service servers in a domain-based environment. When *This domain* is used and the server is also a domain controller, terminal servers that are members of the same domain can locate the license server without any additional configuration. If the server is not a domain controller, the server must be published in AD for terminal servers in its domain to locate it. See the “Publishing a Terminal Services Licensing Server Using TS Licensing Manager” section in this chapter for more information. To select this option, you must be logged on as a domain administrator from the domain in which the computer is a member.

As mentioned, *The forest* wizard option is the recommended setting for TS Licensing role service servers that are domain members. When used, terminal servers that are members of any domain in the forest can locate the license server without any additional configuration. To select this option, you must be logged on as an enterprise administrator from the forest in which the server is a member. A terminal server in a Windows Server 2008 domain will attempt to locate and contact a license server in the following order:

1. License servers that are specified in the Terminal Services Configuration tool or by using group policy.
2. A license server that is installed on the same computer as the terminal server.
3. License servers that are published in Active Directory Domain Services.
4. License servers that are installed on domain controllers in the same domain as the terminal server.

EXAM WARNING

Just selecting the Forest Discovery Scope is not enough to enable a TS Licensing server to issue TS Per User CALs to users in multiple domains. To issue CALs to users of another domain, the server must be added

to the Terminal Server License Servers group in that domain. It's also not necessary for a server to have its discovery scope set to *The Forest* in order to hand out TS CALs in multiple domains, as long as it is a member of this group in each domain it will service. However, by default, only servers in its own domain will be able to automatically discover it.

Using the Terminal Services

Configuration Tool to Specify a TS Licensing Server

Instead of using automatic discovery, a terminal server can be forced to use a specific TS Licensing server.

1. Open the Terminal Services Configuration utility by choosing **Start | Administrative Tools | Terminal Services | Terminal Services Configuration**.
2. If Terminal Services Configuration is not pointing to the correct terminal server, follow steps 3 thru 5. If it is, skip to step 6.
3. Connect to the correct server by selecting **Action | Connect to Terminal Server**.
4. In the **Select Computer** dialog box, choose one of the following:
 - Select **Local computer** if running Terminal Services Configuration on the terminal server you want to configure.
 - Select **Another computer** and click **Browse** if you are not running Terminal Services Configuration on the terminal server you want to configure. In the **Select Computer** dialog that appears, type the name of the server in the **Enter the object name to select (examples):** text area, click **Check Names**, verify the server name, and click **OK**.
5. Click **OK**.
6. In the center pane, right-click **License server discovery mode** and click **Properties**.
7. In the **Properties** dialog box, select the **Use the specified license servers** option.
8. Click the **Licensing** tab.
9. Enter one or more license servers into the provided text box, and then click **Check Names**.

10. A **Terminal Services Configuration** dialog box briefly appears while the names you've entered are being checked. A **Terminal Services Configuration** pop-up box then appears, which notifies you that the names have been successfully verified. Click **OK**.
11. In the **Properties** dialog, click **OK**.
12. In the center pane, verify that the **License server discovery mode** setting has changed to **As Specified**, and then close Terminal Services Configuration.

Publishing a Terminal Services Licensing Server Using TS Licensing Manager

As mentioned previously, when the TS Licensing role service is installed on a server that is a domain member but not a domain controller, it will not be automatically discovered by terminal servers in its domain. In order to make it discoverable, you must publish the server in AD. You must have membership in the local Administrators group on the license server and membership in the Enterprise Admins group in AD Directory Services (DS), or you must have been delegated the appropriate authority in order to complete the following procedure:

1. Open the TS Licensing Manager utility by choosing **Start | Administrative Tools | Terminal Services | TS Licensing Manager**.
2. In the right pane, right-click the server you want to publish and then click **Review Configuration....**
3. In the **Configuration** dialog box, click **Publish in AD DS**.
4. Click **Continue**, followed by **OK**.

TS CAL Types

TS CALs are available in two different types to allow for different licensing scenarios to meet the needs of your organization. These can be purchased in either a *per device* or *per user* model depending on how you plan to configure your terminal applications.

- **Per Device** The first time a device connects to a terminal server, it is issued a temporary license for the duration of that connection. All subsequent connections initiate contact with the TS Licensing service and a per-device TS CAL is assigned if one is not already allocated to that device—and if the license database has available licenses. These licenses can be assigned to any device requesting a terminal session and are valid for workstations,

laptops, handheld devices, and mobile clients, as well as any other physical device able to run the appropriate RDP Client. If no licenses are available for the device, the terminal session will not be allowed to be established.

Device CALs are bound to the physical device rather than the user of the device and are ideal in situations where many users will be using shared equipment to access terminal sessions. This works well for thin clients and kiosk computers where these devices will be using terminal services, but where there are many more users than devices.

- **Per User** When a user makes a request for a terminal session, the Licensing Service is contacted to ensure that it should not be using device mode. If the Licensing Service is in per-user mode, the connection is automatically granted since per-user license assignments are not enforced. The user assignments of the TS CALs are logged so that the network administrator can monitor the license usage and buy additional licenses as appropriate. This can be checked at any time using the TS Licensing Manager tool.

Per-user CALs make the most sense when terminal server applications are to be used by a controlled group of users who might access the applications from many different computers or access methods. This usually translates into a group of roaming users who might need to access an important line-of-business application from the office, home, and on the road.

TS CALs must be activated on the Licensing Server before they are able to be assigned to requesting clients. Normally, this process consists of registering the TS CALs with Microsoft over the Internet, but Web and telephone methods are also available if you do not have a connection to the Internet on the machine hosting the Licensing Service.

NOTE

If you need to move the TS CALs to another server or reactivate them for any reason, you will need to use the telephone activation method since they will be listed as being in service.

Locating Terminal Services Licensing Services

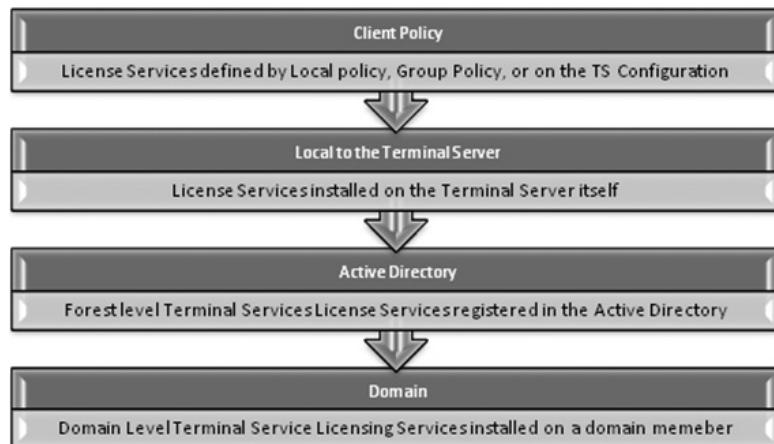
When a client attempts to make a connection to a terminal server, the server must be able to locate a Terminal Service Licensing Service that is able to validate the

license type and provide the appropriate TS CALs. The License Server can apply to three scopes of applications:

- **Workgroup** If your Terminal Server implementation is not part of a domain, this will be the only option available to you. Terminal servers will only be able to find this Licensing Service if they are in the same workgroup as the Licensing Server.
- **Domain** If your terminal server is a domain member, you can configure the Licensing Service at the domain level. Licensing configured at the domain level will be automatically available to all TS Servers in the domain if the Licensing Service is installed on a domain controller. Otherwise, you can specify the location by GPO or by using the Terminal Service Configuration Tool.
- **Forest** The easiest way to configure a TA Licensing Server is at the Forest level. This registers the service in the Active Directory, making it findable by terminal servers anywhere in the Forest. You do have to add the Licensing Server to the Terminal Services License Servers group on each domain you want to be able to use this service before it will be able to assign TS CALs.

Given that a single forest or domain may have several different Terminal Services implementations, each serving different purposes, it should come as no surprise that a single licensing model might not be appropriate in all cases. In these cases, you can use a combination of policies and terminal servers to build a licensing configuration that will meet your needs (see Figure 2.22).

Figure 2.22 Building a Licensing Configuration for a Terminal Services Environment



Configuring & Implementing ...

Common Challenges

A common implementation challenge that you are likely to face involves having different terminal servers for different types of access. For instance, a bank might implement Terminal Services to maintain control of its data and require encryption on any inbound connections using these data. Wealth Managers might need access to a financial planning and forecasting application from anywhere, anytime. At the same time, managers at the mortgage company might need to provide access to a listing application, from just a few terminals. In this case, a single licensing method might not be the most cost effective.

To meet this need, the network administrator installs License Services in per-device mode on the terminal server running the mortgage listing application and a separate forest instance of License Services for all other TS connections. In this case, clients using the mortgage application will receive per-device licenses since they will find the locally installed License Services. All other TS connections in the domain will receive per-user licenses. This helps the organization save money since the two user groups don't overlap.

If you make a mistake in the setup of your TS Licensing Server and need to change the scope of your license service, you aren't stuck. You can easily upgrade a workgroup Licensing Server to a domain server by joining it to the appropriate domain. You can also switch between Domain and Forest scopes through the Review Configuration dialog in the TS Licensing Manager.

EXAM WARNING

Remember the mnemonic C-L-A-D for the order used in locating the TS Licensing Service: Client, Local, Active Directory, Domain controller.

Launching and Using the Remote Desktop Connection Utility

In Windows Server 2008, the application can be opened by choosing **Start | All Programs | Accessories | Remote Desktop Connection**. RDC opens with most of its configuration options hidden. To proceed with the connection type, the name or IP address of the terminal server you want to connect with in the **Computer:** drop-down box, select **Browse for more...** from the drop-down list, or select the server from the drop-down list if you have previously established a session to it, and then click the **Connect** button. If you select **Browse for more...** a **Browse for computers** dialog will appear which allows you to see available terminal servers.

EXAM WARNING

RDC can also be started from a command prompt by specifying its executable file **mstsc.exe**. In Windows Server 2008, the **/admin** option can be used when launching the utility to connect to the server's console session, instead of beginning a new user session. **/admin** replaces the **/console** option used in previous versions. Microsoft stresses this change quite heavily in their documentation. Be sure not to fall for any questions using the older **/console** option. The **/admin** option does not require a TS CAL for connection.

At this point, you might be automatically logged on. Your client may have cached credentials which automatically log you on, a group policy may exist that automatically logs you on with the credentials you logged on to your local computer with, or a similar option may automatically provide credentials for you. If that's the case, a Remote Desktop window will open. If not, the **Windows Security** dialog box will appear asking you to enter a valid username and password. You can also select the **Remember my credentials** box to save your logon credentials for this server. Even if you do not select this box, RDC will remember the username used and automatically offer to use it for subsequent connection attempts. Once you are connected, by default the remote desktop will appear in full screen on your system's display. You can move your cursor over, click, and use any item in the remote desktop just as you would if using your local system. You can also copy and paste between the remote and local computers, using the standard methods of doing this.

Connecting is a simple process; however, terminating your session requires a bit more explanation. Two methods can be used to end your session: logging off

and disconnecting. To log off, click **Start** |  | **Log Off**. When you do this, it will completely log you out of the remote system in much the same way as if you logged out on your local system. Registry entries are properly written, programs are elegantly closed, and so forth. The session is completely removed from the Terminal Services server, freeing up any system resources that were being used by your session. Make sure you select **Log Off**, rather than Shut Down. If you select **Shut Down**, and are logged onto the remote session with rights that allow your account to shut down the server, it will power down. Obviously, this will affect everyone who is currently using it.

The second method of terminating your session is to use the process known as *disconnection*. When you disconnect from terminal services, your session remains on the server and is not removed. It continues to consume resources, although the video stream coming to your local computer and input stream going from your local computer to the terminal services system are terminated. When you launch RDC again and connect to the same server running terminal services, your session will still be there exactly as you left it and you can take up where you left off. This can be helpful in cases where an application is being run that requires lengthy processing. You do not have to remain connected for the application to run and you can check back later and obtain the result. You can disconnect from your session by clicking the close button (the **X**) in the top right corner of the Remote Desktop window, or in the full screen connection bar.

Configuring the Remote Desktop Connection Utility

In the previous section, we simply launched the Remote Desktop Connection utility and established a connection. When you initially launch the utility, most of its configuration information is hidden. To display it before you use it to establish a connection, click the **Options** button. This will reveal a series of tabs and many additional settings that can be configured. Let's take a look at each in the following sections.

The General Tab

The General tab contains the Computer: drop-down box, which holds the names and IP addresses of computers to which you have previously connected, along with an option to browse the network for computers not listed. This tab also contains the User name: text box. The Allow Me To Save Credentials check box will ensure that the credentials you type in while logging on are saved for future sessions. This tab also allows you to save your connection settings. You might have several different terminal servers to which you connect using RDC. If so, it is helpful to not have to configure the utility each time you open it. When you click the Save As... button,

a Save As dialog box opens, asking you where you'd like to save the file that contains your configuration information. The file will be saved with an RDP extension, and can be double-clicked later to establish a terminal session. You can also use the Open... button on this tab to specify that the settings from a previously saved RDP file be loaded into the utility.

EXAM WARNING

Asking RDC to remember your credentials doesn't work on all versions of Microsoft Windows Vista. The following versions of Windows Vista do not support this feature: Home Basic, Home Premium, and Starter.

The Display Tab

The display tab controls how the remote desktop appears on your client computer. The top portion contains a slider that controls the size of the remote desktop that will be displayed on your screen. The maximum resolution supported is 4096×2048 , and the default setting is Full Screen. The next portion of this tab controls the color depth (in bits) of the remote desktop when it is displayed on your local computer. The drop-down list box contains the following options: 256 colors, High Color (15 bit), High Color (16 bit), and True Color (24 bit). Higher color depths require more resources. Note that settings on the server may override your selection.

Finally, the bottom of the tab contains a check box entitled Display The Connection Bar When In Full Screen Mode. When selected, this setting places a small bar at the top of a full screen remote desktop, which makes it easier to size, minimize or maximize (to full screen), or close the Remote Desktop window.

The Local Resources Tab

The Local Resources tab allows you to control whether or not client resources are accessible in your remote session. When you are working in a session, you are actually working on the remote terminal server. This means that when you open Windows Explorer, the disk drives you see are the ones that are physically located on the terminal server, not the ones installed in your local computer. Selections on the Local Resources tab can be used to make your local drives, client-attached printers, and similar client-side resources available for use within your remote desktop session.

The first setting on the tab deals with whether audio will be used in the session. The default setting, Bring To This Computer, allows for any sounds played in the session to be transferred from the terminal server to the client. Audio transfer can be bandwidth-intensive in a thin-client environment, so Microsoft also gives you the opportunity to not transfer this audio. The Leave At Remote Computer setting plays the audio in the session on the Terminal Services computer but does not transfer it to the client. The Do Not Play setting prevents audio in the session altogether.

The next setting on the Local Resources tab relates to whether keyboard shortcut combinations are used by the local operating system or the Remote Desktop window. The three possible settings for keyboard shortcut combinations include:

- **In full screen mode only** In this mode (which is the default), when you use a shortcut combination, the system applies it to the local operating system, unless there is a full-screen Remote Desktop window open.
- **On the local computer** This setting applies all shortcut combinations to the local operating system.
- **On the remote computer** This setting applies all shortcut combinations to the Remote Desktop window.

EXAM WARNING

You cannot redirect the **Ctrl + Alt + Del** keyboard combination. This combination only works on the local operating system. An equivalent that can be used in the Remote Desktop window is **Ctrl + Alt + End**.

The final section of the tab deals with determining which devices from the client system are automatically made available to the user within the remote desktop session. By default, the following are selected: Printers, Clipboard, and Smart cards. The Smart cards option is available by clicking the More... button. Other options that clicking the More... button reveals include Serial ports, Drives, and Supported Plug-and-Play devices. *Drives* can be expanded, which allows you to select the individual drive letters you'd like to have available from your local system. These will not be available with the same drive letters in your terminal session (the server most likely already has a drive C, for example), but will be clearly identified and easy to discern.

New & Noteworthy...

Plug-and-Play Device Support

Windows Server 2008 terminal servers include enhanced redirection support for Plug-and-Play devices that are physically plugged into your local computer but need to be available in your terminal services session. This includes media players that are based on the Media Transfer Protocol (MTP) and digital cameras that are based on the Picture Transfer Protocol (PTP). You cannot transfer digital rights management protected content from redirected media players to a terminal services session. To enable redirection, in the RDP utility click the **Local Resources** tab, followed by the **More...** button. Expand the plus (+) sign next to **Supported Plug and Play devices** to see all devices attached to your system that will work with this feature. If you have Plug-and-Play devices attached to your system that do not show up, they are not compatible with Terminal Services Plug-and-Play device support. Plug-and-Play redirection only works for clients running Windows Vista Enterprise or Ultimate.

The nature of Plug-and-Play devices is that they are not always connected to your computer. You might be wondering how Terminal Services deals with devices that are plugged in during an active Terminal Services session. Microsoft considered this when designing this functionality and provides an option under **Supported Plug and Play devices** called **Devices that I plug in later**. By default, neither **Supported Plug and Play devices** nor **Devices that I plug in later** are selected. By selecting these options, any compatible Plug-and-Play devices you plug into your local system during an active Terminal Services session will be detected and made available not only on your local system but also in your Terminal Services session.

TEST DAY TIP

Make sure you are familiar with new features such as Plug-and-Play device support. New components that relate directly to test objectives are likely to be featured in exam questions.

The Programs Tab

By default, when you connect to a Terminal Services session, you will receive a Windows desktop. The selections on this tab allow you to receive a specified application instead of a desktop. If Terminal Services is being used to provide only a single application for each user, this setting can increase security by ensuring that users do not receive a full desktop upon connection. This will prevent them from performing tasks on the server other than running the specified application. If the check box next to Start The Following Program On Connection is selected, only that application will be available in the session.

Selecting this check box enables the Program Path And File Name: text box. If the path to the application is already contained in one of the Windows path variables on the Terminal Services computer, you can just type the name of the application's executable file in this box. If not, you must include the full path and filename of the executable. The check box also enables the Start In The Following Folder: text box. If the application requires the specification of a working directory, enter it here. This is often the same directory in which the application is installed.

After the connection is made with a specified program starting, the traditional methods of ending your session (discussed previously) will not always be possible. Most programs have an Exit command on a menu, embedded in a button, or contained in a link. When you have specified an initial program, the Exit command is the equivalent of logging out. To disconnect, simply close the Remote Desktop window.

The Experience Tab

The Experience tab allows you to customize several performance features that control the overall feel of your session. All of these settings except Bitmap Caching can generate substantial amounts of additional bandwidth and should be used sparingly in low bandwidth environments. Not all features are available for all client operating systems. The check boxes on this page include the following:

- **Desktop background** Allows the background image of the desktop (wallpaper) in the remote session to be transferred to and displayed in the Remote Desktop window on the client.
- **Font smoothing** Enables ClearType font support in a Terminal Services session.
- **Desktop composition** Enables the session to display the visually dynamic features, known as Windows Aero (such as translucent windows), implemented in Windows Vista. The client hardware must support this option, but the server does require compatible hardware.

- **Show contents of window while dragging** Rapidly refreshes a window so its contents are visible as the user moves it around the screen in the Remote Desktop window.
- **Menu and window animation** Enables some sophisticated effects, such as the Windows Start menu fading in and out, to be displayed in the Remote Desktop window on the client computer.
- **Themes** Enables any themes used in the remote session to be enabled and transferred to the Remote Desktop window on the client.
- **Bitmap Caching** Enables bitmaps to be stored locally on the client system and called up from cache, rather than being transmitted multiple times across the network. Examples of bitmaps include desktop icons and icons on application toolbars.

At the top of this tabbed page is a drop-down box that contains several pre-defined combinations of these settings that Microsoft has optimized for different levels of available bandwidth. Table 2.3 shows which bandwidth level corresponds to which settings.

Table 2.3 Preconfigured Bandwidth Settings

| Connection Speed Selection | Desktop Background | Font Smoothing | Desktop Composition | Show Contents of Window while Dragging | Menu and Window Animation | Themes | Bitmap Caching |
|---------------------------------|--------------------|----------------|---------------------|--|---------------------------|--------|----------------|
| Modem (28.8 Kbps) | | | | | | | X |
| Modem (56 Kbps) – default | | | | | X | | X |
| Broadband (128 Kbps – 1.5 Mbps) | | | X | X | X | X | X |
| LAN (10 Mbps or higher) | X | X | X | X | X | X | X |
| Custom | | | | | | X | X |

The Experience tab also contains a check box entitled Reconnect If Connection Is Dropped, which is selected by default. Windows Server 2003 and later versions of Terminal Services include the automatic reconnection feature. If dropped packets, network service interruptions, or other network errors cause your Terminal Services connection to disconnect, this feature will automatically attempt to reconnect to your session without requiring you to reenter your logon credentials. By default, there will be a maximum of 20 reconnection attempts, which occur at five-second intervals. Generally, a notification message will pop up, informing you that the connection has been lost and counting down the remaining connection attempts.

The Advanced Tab

The top of this tab allows you to configure Server authentication options. Server authentication is an extra level of security that is used to verify you are connecting to the intended terminal server. It contains three possible settings. The default, Warn me, notifies you if the authentication fails but still allows you to connect if desired. The option Connect And Don't Warn Me will silently connect you to the terminal server even if RDC cannot verify the identity of the server. The final option, Do Not Connect, notifies you and will not allow the connection to proceed. Windows Server 2003 SP1 and earlier servers that cannot provide the type of authentication requested should be set to Connect And Don't Warn Me. Later servers that can provide this authentication information should be set to one of the other options. The bottom of the Advanced tab, Connect From Anywhere, allows you to configure TS Gateway connection settings.

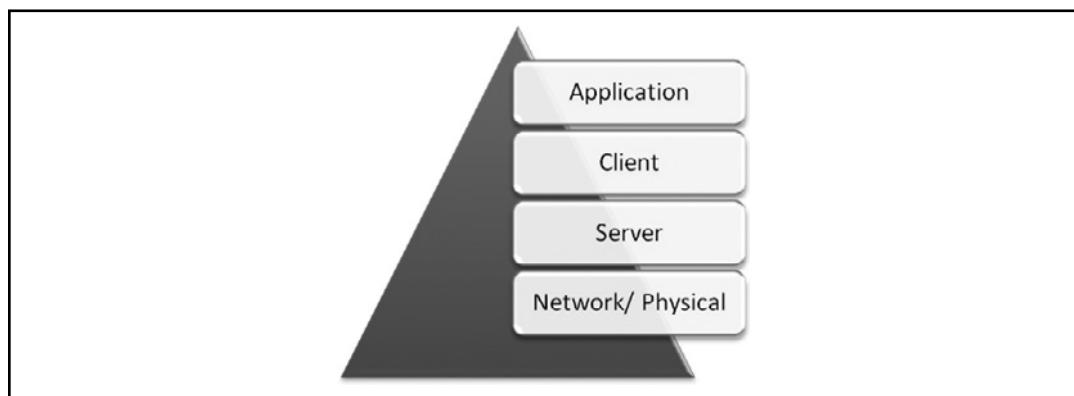
Terminal Services Troubleshooting

Windows Server 2008 has made many improvements to Terminal Server both in expanding the functionality of the product as well as improving the stability and availability of the service to the end user. With the addition of the Session Broker, terminal servers can now work as teams coming together as server farms able to provide continuous service. This means that a problem on a single server doesn't necessarily translate to an outage of the service. The remaining servers in the farm can continue while the ailing one is repaired. Moreover, this gives the network administrator the opportunity to schedule outage windows for upgrades and maintenance that don't have to have a direct impact on application availability.

When legitimate trouble does arise though, it is important to take immediate action to track down the source of the problem and resolve it quickly. Because Terminal Server uses shared hardware, the scope of effect of a small problem can be rather large, affecting dozens of users at once or even an entire population of users for line-of-business applications.

It is important to have a sound methodology in place to help you troubleshoot problems quickly and to isolate problems on the network. Simply restarting a server or asking a client to log in again doesn't help isolate problems and can often lead to problem masking or workarounds that can become embedded in your business and, once in your corporate culture, can lead to bad habits that your users will keep for years. When you are attacking problems, it is usually easiest to follow the building-block approach, starting at the bottom of the pyramid and working upward (see Figure 2.23).

Figure 2.23 Solving Network Problems



- **Network/Physical** At the physical layer, it is important to verify that there are no hardware problems with your servers and that they are able to communicate on the network. This might seem like a trivial step, but servers do get accidentally turned off, power grids fail, and remote network connections can be cut.
- **Server** At the server layer, it is important to validate that there are no underlying issues with the terminal server and that the operating system is functioning as expected. It is at this layer that event logs should be checked for problems and services monitored to be sure that they are functioning properly.
- **Client** At the client level, the terminal settings should be verified and the authentication checked to be sure that the client is correctly working with the Terminal Server. Client logs should also be checked to surface any problems here that could be causing the disruption.
- **Application** Finally, at the application level, specific compatibility and performance issues should be checked to ensure that there are no issues with the underlying application install. In the case of remote applications,

it is also important to be sure that there have not been any untested patches or system configuration changes that could lead to the problem.

As you can see, tackling a troubleshooting challenge should be done in the order of impact to triage problems that could impact the largest number of users (the terminal servers have lost power) to the smallest impact (a single application is experiencing performance problems). As you work through these steps, it is important to keep an activity log so steps are not duplicated and to ensure that you methodically work through all components involved to narrow the problem down to its root cause.

A number of tools are available to the network administrator to help in the troubleshooting of the Terminal Services components. These should be used to gather additional information about the state of the system and to outline problems in the individual components that could be contributing to a larger problem.

- **System Event Logs** While not directly aimed at the management and maintenance of Terminal Services, the System Event Logs can provide a first warning of problems on your servers and supply additional details to track specific errors.
- **Terminal Services Manager** The Terminal Services manager allows the network administrator to see the current utilization of a single terminal server and to manage the connections attached to it. It is from here that you can disconnect broken connections, communicate with currently connected users, and view session idle times.
- **TS Gateway Console** The Gateway console can be used to track connections that are being routed through the gateway and to track the number and types of sessions that are active. In a larger environment, where many different terminal servers are used through a single gateway, the Gateway console can provide a single picture of the remote TS utilization across the enterprise.
- **WSRM** The Windows System Resource Manager (WSRM) is an advanced management application that allows a network administrator to tailor system memory, disk, and processor power across a number of different Terminal Services applications according to business priority.

For instance, in an environment where resources are at a premium, a mission-critical financial package could be given processor priority over all other applications to ensure that the impact to the business is minimized as the terminal server comes under high load. WSRM essentially acts to enforce a service level on a terminal server that is driven by business rules.

- **Terminal Services License Manager** It is important for a network administrator to be able to track and manage the TS CALs that are in use on the corporate network. The TS License Manager can display the current licenses that have been allocated and help plan for future scalability.
- **Performance Monitor** The performance monitor is a monitoring tool that will be familiar to network administrators who have used previous versions of the Windows Server Platform. PerfMon can gather general server statistics to display problems with memory, disk activity, and processor utilization that can plague a poorly designed or oversubscribed terminal server.

Routing and Remote Access

Users are accustomed to being able to work and reach network resources when directly connected to the corporate network, but the increased mobilization of workforces and additional time and travel demands are rapidly increasing the need for true ubiquitous computing. This means users need to be able to access appropriate corporate data, services, and resources whether they are in the office, on the road, at home, or even on nontraditional mobile devices.

This need introduces several logistic and security problems not present on the relatively closed system that makes up the corporate network. In a traditional network, much of the security can be controlled by the domain membership of the local workstations that allows the network administrator to build group policies to control configuration and user rights. Remote workstations and devices are not necessarily members of the domain and might have other applications and security holes that would not be permitted on a corporate network. These devices introduce security risk since when they connect to the corporate network, they bring with them all of the potential risk on the single machine, extending the surface area of attack outside of the network boundaries.

Such remote access risks include:

- **Exposure to Malware** If the connecting device does not have appropriate antivirus software or has not been appropriately updated, this external machine can act as the entry point for the virus. Any perimeter security or edge filtering that the network uses will effectively be circumvented.
- **Point of Least Security** In cases where the remote workstation has been misconfigured or has not been updated with the appropriate security patches, the vulnerability to the single workstation might be passed on to the internal network. In this case, it makes the remote device the weakest link in the corporate security strategy and brings unanticipated risk.

In addition to the risk to the host network, there is also additional risk to the data as it is leaving the corporate environment and being transmitted across the public Internet. It is important that the integrity of the data that are transferred be maintained and that the data really does get delivered to the intended destination.

Data transfer risks include:

- **Impersonation** In this scenario, a third-party will pretend to be a valid client on the network. This might be done by capturing valid credentials or by listening to the authentication process and playing that communication back to the server in hopes that the server will allow the authentication.
- **Man-in-the-Middle** In this scenario, a third party will intercept the data stream in both directions and will pass the data through, maintaining a copy of the data to be shipped elsewhere or used for other purposes. The client and the server think they are talking directly to one another and never see the interception.
- **Data Replacement** This is similar to a Man-in-the-Middle attack, but that the interceptor is an active participant and might change data in the communication during transit so that the result of the communication is changed.
- **Denial of Service (DoS)** In this scenario, a third party acts to prevent network traffic from being passed between the internal resources and the clients. This can lead to expensive downtime and lead to a disruption of the business.

With all of these potential risks, you might be tempted to not allow users to remotely connect to the network. While some network administrators have certainly taken this stance, it does not generally support the business well and carries a real cost since users will often find a way around this kind of limitation, bringing even higher risk to the network and, even worse, risk that users will actively keep from the network administrators.

Head of the Class ...

Have a Remote Access Strategy in Place

Users who have a legitimate business need will often find a way to work around IT rules. Worse still is the fact that they'll often get organizational

Continued

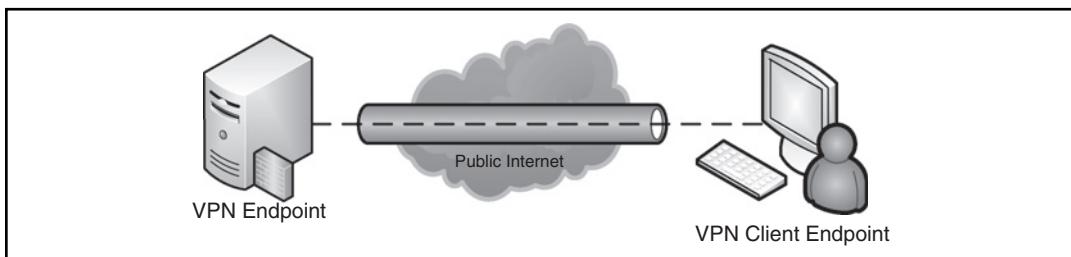
support if the need is real. It is generally better to work with users to accomplish their goals than to have an arbitrary policy.

Rather than having users begin to use insecure third-party Web-enabled remote desktop applications under the radar, it is better to have a planned remote access strategy with appropriate security controls. It is more defensible to tell users that they need to abide by a corporate access policy enforced by NAP than to deny access completely.

Virtual Private Networking

The creation of virtual private network (VPN) connections is the answer to both access and data transfer risks. Using a VPN, a remote workstation can authenticate to the domain and establish a secure tunnel between the private corporate network and the remote device over public networks like the Internet (see Figure 2.24). This tunnel security is further enhanced by the integration of NAP authorization to the VPN negotiation, allowing the network administrator to be able to control the security of the connection as well as the health requirements of the workstations.

Figure 2.24 A VPN Connection



A number of different technologies or protocols can be used to establish a VPN between clients and the corporate network. Each of these has benefits and challenges, but the choice of technology will largely be determined by the control the system administrator has over the client computers and the security requirements that must be followed for VPN communications.

VPN Authentication Protocols

In order for a VPN connection to be successfully established, both ends of the tunnel must be speaking the same language (protocol) and must agree on how they will

negotiate the connection. Principle of these is the Authentication method they will use to identify the initiator of the tunnel so the VPN server can make the associated Authorization that the initiator is allowed to communicate on the VPN. Several common authentication methods can be used in establishing the tunnel, such as:

- **Password Authentication Protocol (PAP)** This is the most fundamental of authentication methods. Under PAP, passwords are sent across the wire in unencrypted text form as either user credentials or as a shared secret (connection password). Because this traffic is susceptible to being captured in transit, this method is almost never used.
- **Challenge-Handshake Authentication Protocol (CHAP)** The CHAP protocol is a bit better than PAP in that it does not send the user's password across the network unencrypted, though it does require that both parties know the unencrypted password. In this protocol, the server sends an arbitrary (Challenge) string to the client. The client responds by returning the clear-text username and a hashed version of the Challenge string, session ID, and password using the MD5 hash protocol. The server compares the hashed value with the expected result for the username and, if they match, allows the connection.

The strength here lies in the fact that the challenge string is arbitrary so that playing it back will not result in a hacker gaining access to the system. It should be noted, though, that the MD5 protocol is considered hackable and should not be used in high-security environments.

- **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)** This is a Microsoft version of CHAP that includes control and feedback features as well as additional security features. This version allows the servers to rely on encrypted versions of the passwords so that neither end of the tunnel need be aware of the unencrypted passwords.
- **MS-Chap v2** This is an updated version of MS-CHAP that requires mutual Authentication. That is, each side of the tunnel will send a challenge string to the other requiring a correct response before the authentication is complete. This is a much more secure implementation in that it requires the server to authenticate the client and the client to authenticate the server. MS-CHAPv2 also provides additional keys and control information to handle more advanced data encryption across the tunnel.
- **Extensible Authentication Protocol (EAP)** EAP is a framework that acts as an authentication platform rather than authentication itself.

This allows VPN endpoints to negotiate authentication, which can include Active Directory, certificates, or RADIUS among others.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) has been a VPN standard included in Windows operating systems since Windows 95 OEM Service Release 2 (OSR 2). This protocol has been used in many corporate implementations and was the *de facto* standard for many years, although it has generally been replaced by the L2TP/IPSec protocols. It is still chosen for its ease of configuration and backwards compatibility in some applications.

The PPTP protocol relies on two simultaneous connections to function. First, a Generic Routing Encapsulation (GRE – IP Protocol 47) tunnel is made to provide a standard PPP (Point-to-Point Protocol) connection. A second connection is made on TCP/1723 to provide control information for the GRE tunnel.

Prerequisites

In order to use PPTP, the client and server VPN endpoint must be able to communicate directly and establish connections on both GRE and TCP/1723. All clients involved in these communications must be Windows 95 or newer.

Pros

Here are some of the benefits of using PPTP:

- **Compatibility** The PPTP protocol has been a staple of the VPN and RRAS components of Windows for many years and has a wide installation. Because of its longevity, most network administrators have some experience with PPTP and the configuration of this kind of tunnel.
- **Ease of Use** The configuration of a PPTP connection is relatively easy and does not require a complicated setup and prerequisites to bring it alive.
- **Traffic Diversity** Because PPTP uses a GRE tunnel, almost any kind of network traffic is eligible for traversal through the tunnel. This includes TCP/ IP traffic, Multicast, and IPX.
- **Traffic Compression** This protocol can make use of the Microsoft Point-to-Point Compression (MPTPC) protocol.

Cons

Here are some of the drawbacks related to using PPTP:

- **Firewall Traversal** Because multiple sessions are involved in the establishment and control of the PPTP tunnel, this is not usually an option when either endpoint is behind a modern firewall doing deep inspection.
- **Security Concerns** Much of the network traffic sent across the wire in the establishment and maintenance of the tunnel is unencrypted. Once the tunnel is established, the transferred data are encrypted, but capture and analysis of the initiation dialogue can lead to the tunnel being compromised or spoofed.
- **Connection Passwords** In circumstances where the PPTP tunnel is established with Shared Secrets, the passwords for the tunnel can be guessed by brute force methods.

PPTP can be an appropriate VPN protocol where simplicity in design and broad compatibility are primary design constraints. The lower implementation barrier is commensurate with the lower security and lack of advanced configuration options. Still, PPTP works well for temporary client connections rather than more permanent network-to-network connections.

L2TP/IPSec

L2TP/IPSec is a combination of two technologies, Layer-2 Tunneling Protocol (L2TP) to establish the tunnel and IP Security (IPSec) for encryption. This is generally considered a replacement for PPTP, providing better encryption and more complete authentication.

Prerequisites

Implementation of IPSec in the environment will generally require that a Certificate Authority be implemented to issue user or computer certificates for the authentication process. You'll also need to make sure your firewall is able to support NAT Transversal.

Pros

Here are some of the benefits of using L2TP/IPSec:

- **Completeness of Encryption** IPSec encryption begins before the PPP session is established, encrypting the entire communication exchange and negotiating the user-level authentication.

- **Multiple Authentication Methods** In addition to user authentication, certificate-based computer authentication is also required to establish the connection.
- **Advanced Encryption** These kinds of VPNs are able to use DES and 3DES encryption to secure data transfer rather than the older RSA algorithms.

Cons

Here are some of the drawbacks related to using L2TP/IPSec:

- **Reliance on UDP** The User Datagram Protocol (UDP) is used to pass data into the L2TP protocol. This protocol does not track delivery and might result in retransmission on the network leading to additional overhead.
- **Complexity of Technology** Implementation of IPSec requires computer certificates and the infrastructure to support them. This might require an organization to implement Certificate Authorities (CAs) or a full-blown Public Key Infrastructure (PKI).
- **NAT Issues** By default, IPSec cannot cross boundaries created by firewalls employing Network Address Translation (NAT). While NAT is used in almost all corporate networks, a feature called NAT Transversal (NAT-T) supports the passage of IPSec across the NAT. This is sometimes considered a security risk and should be considered within a larger security plan.

L2TP/IPSec provides a robust combination of tunneling with advanced encryption. This is especially suitable for corporate environments that have already invested in a PKI or that have the need to establish long-term network-to-network connections bridging branch offices with a central hub.

SSTP

The Secure Socket Tunneling Protocol (SSTP) is a new addition to the suite of remote access protocols available to the Windows platform. With both PPTP and L2TP/IPSec, special considerations must be taken to ensure that the appropriate traffic can pass through the corporate firewalls to reach the other VPN endpoint. SSTP provides a high level of security while also being almost transparent to firewalls.

Prerequisites

Because the SSTP protocol makes use of the Secure Sockets Layer (SSL) protocol, the corporate firewall must be able to accept traffic on the HTTPS port (TCP/ 443). SSTP also requires Windows Server 2008 and Vista SP1

as its endpoints, and additional PKI infrastructure may be needed to support advanced authentication criteria.

Pros

Here are some of the benefits of using SSTP:

- **Able to Function over SSL** SSTP is able to use the common SSL port to send communications through firewalls and NAT boundaries, making it much more transparent to the physical network over which it passes.
- **High Level of Security** All of the advanced authentication protocols are supported, and certificates are used to establish SSL connections and initiate VPN connection data.
- **Native Support for IPv6** The SSTP protocol supports both the standard IPv4 and IPv6 addressing and traffic out of the box, without any additional updates or support.
- **Integration with NAP** This protocol was built from the ground up with NAP in mind and is not a retrofit of older technology into the new security paradigm.

Cons

Here are some of the drawbacks related to using SSTP:

- **Requires Server 2008 and Vista SP1** Implementation of SSTP requires that both server and client endpoints be the latest windows versions without the ability to bring legacy clients into the communication.
- **Requires Certificates** These will be required both for the establishment of the SSL session but also for additional authentication that might be done through EAP. This may require a combination of public certificates and certificates issued through an Enterprise CA.

The SSTP protocol simplifies the configuration and network considerations involved in establishing VPN connections with no compromises in security. This does, however, come at the cost of losing backwards compatibility. SSTP remains a strong choice for environments that can tightly control the client and server infrastructure and that have made the investment in strong security standards where integration with NAP is important.

EXERCISE 2.6

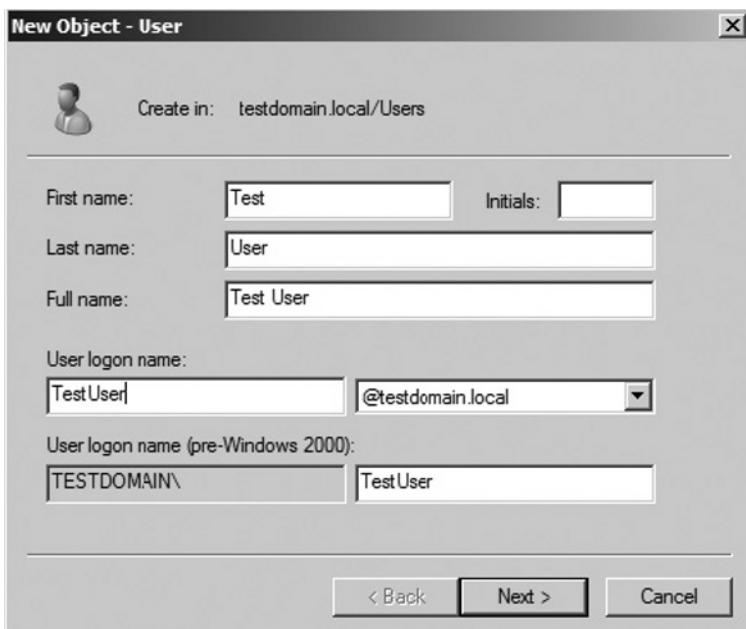
CONFIGURING VPN CONNECTIONS

This exercise assumes a domain environment with Enterprise Certificate Services installed, and with Web enrollment and NPAS already installed. In a production environment, this would not be done on a domain controller to maintain appropriate domain security.

To create a test user with Remote Access Permissions, follow these steps:

1. Log on to your domain controller with Administrator privileges.
2. Navigate to **Start | Administrative Tools | Active Directory Users & Computers**.
3. Expand the **Domain** node and click the **Users** container.
4. Click the **New User** button.
5. Enter a username of **TestUser** (see Figure 2.25) and then click **Next**.

Figure 2.25 Configuring VPN Connections



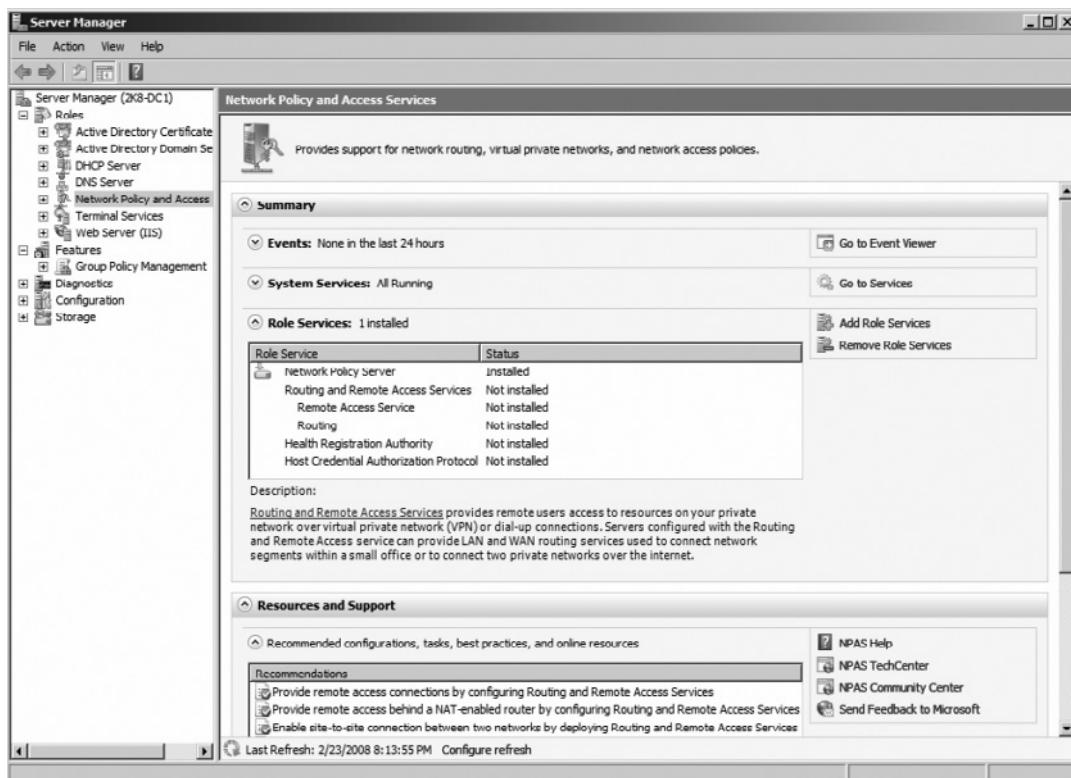
6. Enter a password of **Password1** and click **Enter**; then click **Finish**.

7. Double-click the newly created user to access the properties page.
8. Click the **Dial-in** tab at the top of the properties screen.
9. Select the radio button for **Allow Access** and then click **OK**.

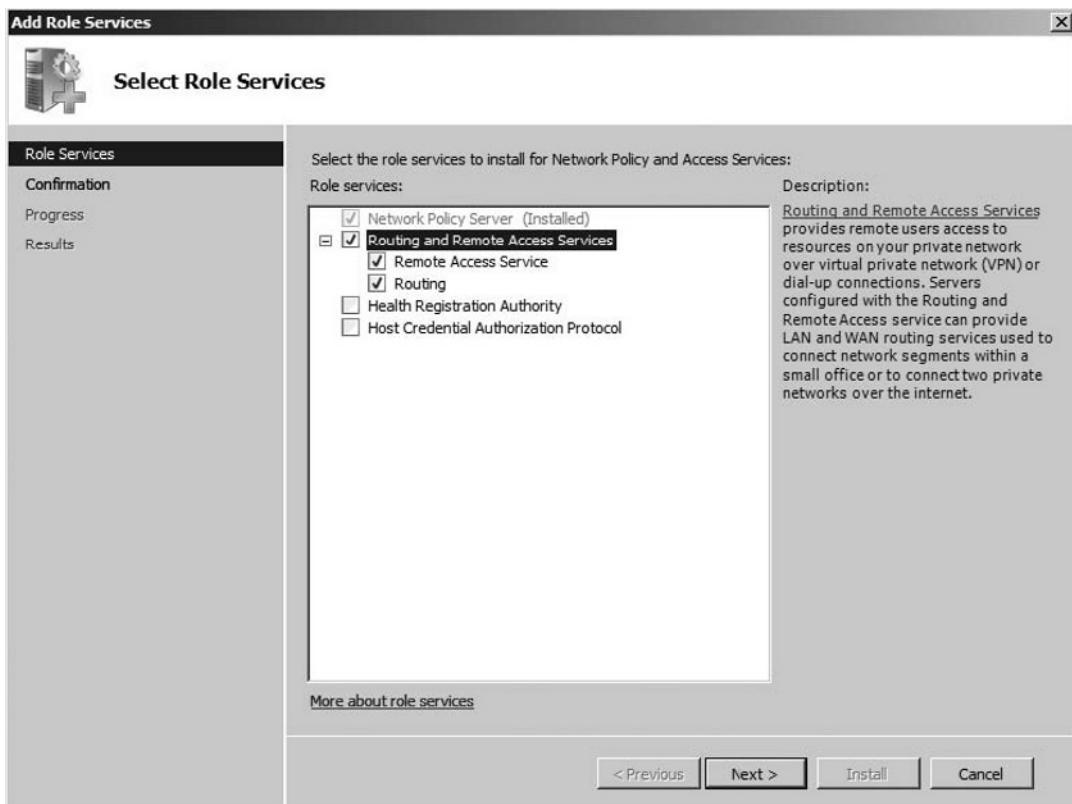
To install routing and remote access services, follow these steps:

1. Navigate to **Start | Administrative Tools | Server Manager**.
2. In the left pane, select **Network Policy and Access Services**.
3. Under **Role Services**, click **Add Role Services** (see Figure 2.26).

Figure 2.26 Server Manager



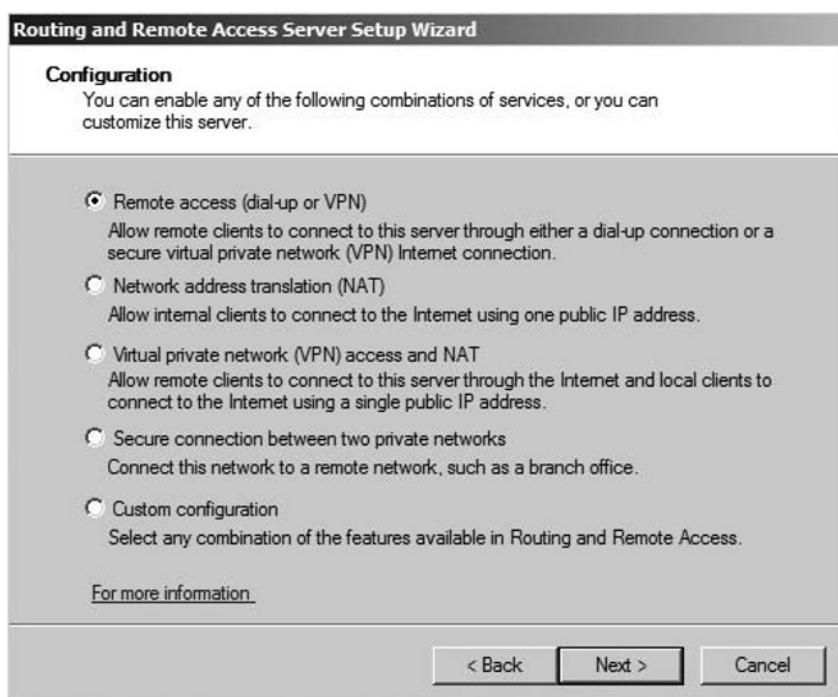
4. Select **Routing and Remote Access Services** (see Figure 2.27). Click **Next**.

Figure 2.27 Selecting Role Services

5. Validate the settings and click **Install** to confirm the install options.
6. Click **Close** to complete the installation.

To configure VPN services, follow these steps:

1. Navigate to **Start | Administrative Tools | Routing and Remote Access**.
2. In the left pane, you'll note that the server has a red "down" icon next to it. Right-click the server and choose **Configure and Enable Routing and Remote Access** to start the server setup wizard.
3. Click **Next** to begin the configuration.
4. On the **Configuration** screen, select the radio button for **Remote access (dial-up or VPN)**. Click **Next** (see Figure 2.28).

Figure 2.28 The Configuration Screen

5. On the Remote Access page, select the check box for **VPN** leaving the Dial-up box clear. Click **Next**.
6. On the VPN Connection page, select the Public NIC in the server. Click **Next**.
7. Specify an IP range for client connections and click **Next** twice.
8. Click **Finish** to complete the installation.

The server is now configured to accept VPN connections from users.

Monitoring and Maintaining NPAS

With all the effort that you have put into carefully planning and implementing your network access solution, it is important that it continue to work in a reliable and responsive manner. Just as with any technology, a certain level of “care and feeding” is necessary to ensure that the environment continues to be trouble-free and easy to operate. Conversely, allowing your network access solution to grow organically without any maintenance will allow uncertainty to creep into the system that is specifically designed to eliminate these kinds of security problems, leading to overhaul upgrades every time changes have to be made to the system.

A number of tools are available for the monitoring and maintenance of the Network Policy and Access Services:

- **NPS MMC Console** Through this snap-in, all of the NPS configurations and rules that have been configured on the network are documented here and can be disabled or enforced through this console.
- **GPMC** The Group Policy Management Console (GPMC) provides a single view of the group policies in force and allows the network administrator to plan and test the deployment of IPSec policies to tailor the security experience that the end user will see.
- **RRAS MMC Console** This snap-in is responsible for providing access and status for all of the Remote Routing and Access Services configurations. From here, routing and VPN connections can be configured and viewed.
- **Netsh Commands** A number of commands are available for the management of NPAS from the command line. These can be used to provide full configuration and access into the services for use with scripting or in a Server Core configuration.
- **Windows Firewall with Advanced Security** The WFAS console provides a monitoring feature that can display the current effective firewall rule set as well as a breakdown of the currently enforced IPSec policies.

Working with Perimeter Networks

When planning a network access strategy, it is important to not only evaluate the overall risk to the data you will be moving across your network, but also evaluate the integrity of the network as a whole. For example, the risk to a Web server running IIS for your company's intranet is dramatically different than the risk to an externally exposed Web server hosting your corporate Web site. This is because the target audience is dramatically different in each case. On the intranet, you can more reasonably assume that the user is going to be bound by company acceptable use policy (AUP) and will not actively be trying to compromise the site. Publicly facing sites have to face a much different landscape comprised of hackers and automated bots in addition to legitimate Web users. Clearly, a very different standard of security must be met that is dependent upon the target audience and exposure to the outside world.

This exposure can be thought of in terms of the surface area of attack. That is, the parts of the system that are available to the outside world over which a connection can be initiated. This could be an open port that is legitimately listening for inbound connection requests (Port TCP/80 for HTTP connections), a remote

access server (VPN Server or TS Gateway), or even a dial-up server taking connections over a phone or ISDN line. The goal is to provide the smallest surface area of attack possible, while still allowing legitimate users to function.

In a very simple network where there is only one segment, all of the servers and users are grouped into a single area. In this case, connections would be passed directly to the inside from the Internet. This is especially dangerous since if one server is compromised or taken over, the hacker or malware would have a platform on the inside of your network from which to launch additional attacks, and any password or network information found on that one machine could be translated into credentials networkwide. This risk has led to the development of perimeter networks—also called demilitarized zone (DMZ) networks—to segment internally available servers (corporate servers) from externally available servers (bastion servers).

This means that even if all of the servers in the perimeter network were compromised, the integrity of the internal network would be preserved, providing a buffer between the outside world and your corporate network. Additionally, any data that might be captured or sent out would only be a subset of the data needed by the DMZ servers to function. The appropriate use of perimeter networks can help ensure that your data remain private and that your business continues to function.

Head of the Class...

Follow the Access Path

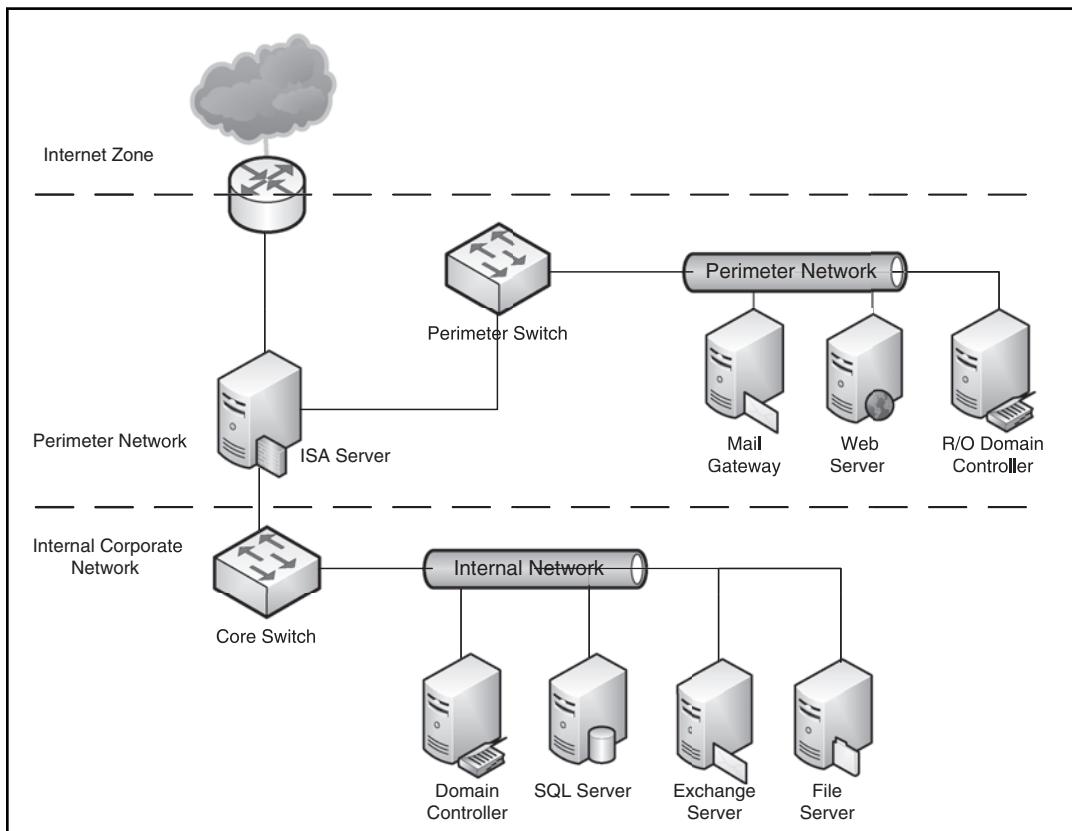
When you are trying to decide if a server or service belongs in the Perimeter network segmented away from the internal network, a good rule of thumb is to follow the access path and how the organization sees the device. In most cases, if a server or application is driving an external revenue stream, this server should be segmented off into the perimeter. This means that eCommerce servers, Web servers, and B2B portals will all likely have some component in the perimeter that acts as the front end to the application where the business processing and data access portions are further protected in the internal network (see Figure 2.29).

Continued

This protects the customer-facing servers from problems on the internal network, allowing them to be managed to a different schedule and set of criteria. This also ensures that these servers don't keep data long. Should one of them become corrupt or be compromised, private data are not stored on them and cannot become an embarrassing news story about identity theft.

Careful implementation of a perimeter network using proper AAA and network access controls is well worth the time spent in planning and testing, and can potentially save your organization time and money over the lifespan of the solution.

Figure 2.29 Perimeter and Internal Networks



Understanding Perimeter Networks

A number of components are involved in the design and implementation of an effective perimeter network. It is easy to focus too tightly on any individual aspect

of security while forgetting the overall goal: to provide IT services to internal and external customers in a secure and reliable way. To do this, it is important to use the Principle of Least Privilege as the guiding principle—that is, to provide the most restrictive access that still allows the customer to be able to access the required data or business functionality. The Principle of Least Privilege can be approached in two ways:

- **Implicit Permit** Under this implementation, base configurations are changed to specifically exclude rights, services, or permissions that are not needed in the final solution. This strategy is often taken when bringing an existing environment into a more secure state, where a system audit might be performed and specific steps taken to remediate known security risks. Anything that has not been explicitly removed by the network administrator is available on the network.

This is often a long and complicated process and is prone to errors since there can be gaps in the analysis portion of the configuration or factors in the environment that are unknown at the time of the implementation.

- **Implicit Deny** Under this implementation, the goal is to start with nothing and build network functionality from there, only implementing systems, services, and permissions that are explicitly needed. This strategy offers a great number of benefits, but it can also be more of a challenge to implement since it requires a thorough understanding of the user requirements as well as the IT systems supporting them.

This is the model that Microsoft has implemented in server 2008 in requiring that server roles be added individually to support user needs. This strategy has the benefit of being more complete since it does not rely on assumptions in the functionality provided to end users. This also can become an easily documented process, because every enabled functionality should be tied to a user request or design requirement.

EXAM WARNING

The Principle of Least Privilege dictates that a user or system should only be granted the minimum privileges required to perform a particular function.

Developing a Perimeter Network Strategy

When taken on a larger scale, the Principle of Least Privilege can be directly applied to the design goals of a perimeter network and its very different user groups, each with their own needs. Internal business users want fast reliable access to services and data and are easily authenticated since they are participating in the full corporate network. External users want access to their appropriate services, but are not as tightly integrated with corporate identity and permissions. Network administrators want to appropriately control access to resources and ensure that they are readily available, but that the risk of compromise or unauthorized access is mitigated. From these diverse needs, the design of the perimeter network is born, separating internal resources from publicly available ones and segmenting data to reduce risk.

Components of a Perimeter Network

- **Firewall** The firewall acts as a security boundary between the different network segments controlling what access is available from one network to another. This device or server inspects packets to match the source and destination tags on packets to ensure they don't violate any of the security rules in place.
- **Network Address Translation (NAT)** NAT provides for the mapping of one network's address into another so that users from one network are able to participate in another. In the case of a Web server in the perimeter network, NAT would be responsible for translating IP addresses to the outside world that would allow the private resource to be found and used by Internet users.
- **Access Lists** These are the specific rules that govern what types of traffic are permitted between the different segments on the network. An access list might allow only Web traffic (TCP/ 80) to reach a perimeter Web server from the Internet, but would allow internal users to access that same server for FTP file transfers (TCP/ 21).

Benefits of Server Core

Because of the potential security concerns in a perimeter network, it is important to reduce the surface area of attack as much as possible. Even with the base Windows Server 2008 implementation, many services are installed by default before any server roles have been implemented. These can be entry points for a hacker or malware should there be a configuration problem, missing patch, or inherent security flaw in the system. Eliminating some of these services lowers the risk and exposes less to the outside world.

Server Core Services

- **IIS Web Services** Server Core is able to provide Web services within the IIS environment with the exception of ASP.NET services.
- **Active Directory Domain Services** Server Core is able to provide comprehensive Active Directory configurations from the command prompt without the overhead of the GUI.
- **LDAP Services** The Lightweight Domain Services are available to meet directory service needs that do not require the full Active Directory implementation.
- **File Services** File shares with full permissions management are available to Enterprise and Datacenter versions of Windows Server 2008, though limited functionality is available on the Standard edition.
- **Dynamic Host Configuration Protocol Services** DHCP IP addressing and remote configuration services are fully supported on the Server Core environment.
- **Domain Naming Services** Full DNS services are supported to provide naming and lookup for Active Directory and general network applications.
- **Print Services** Printer configuration and sharing services are available and for network use.
- **Hyper-v** Full server virtualization is supported in versions of the Server Operating System licensed for the Hyper-v engine.



EXAM WARNING

Server Core is not a command-line application running on the Windows Platform. Instead, it is the fully functioning OS core running without the GUI or other non-essential components.

Server Core is an implementation of Windows Server 2008 that is pared down so as not to run any unnecessary services. This includes the Graphical User Interface (GUI) and many of the management consoles. This has the benefit of eliminating points of attack, but does move the burden to the network.

administrator as all configuration must be done from a command prompt or remote console. This requires a deeper knowledge of the products making this a double-edged sword—very experienced administrators can finely tune security to protect the environment, whereas new users of the command-line tools might introduce new problems as they learn the tools.

In a perimeter network, server core does an especially good job at providing core Internet services such as Internet Information Server (IIS), Domain Naming Service (DNS), and application services.

Using Windows Firewall with Advanced Security

The Windows Firewall with Advanced Security is a hybrid of a more traditional system firewall with IPSec management combining the two technologies into a single platform. When you think about it, the overall goals of the two different technologies are complimentary. IPSec controls the security and authentication of connections with other computers while the firewall controls what kinds of traffic can be pushed across that link. Bringing these two technologies together allows the system administrator to deal with connection security as a single entity rather than having a separate tool for each technology involved.

CONFIGURATION AND IMPLEMENTATION

Several tools are available for the management of firewall security rules:

- Windows Firewall and Advances Security tool
- Domain and Local GPOs
- Command Line (Server Core): netsh advfirewall

Connection Security Rules

IPSec tunneling is used to provide authenticated connections between network endpoints in the corporate environment to implement secure communication and encryption rules on the network. By default, there are no rules implemented, but these can easily be configured to meet business needs. Several different types of Connection Security Rules can be set up, including:

- **Isolation** These rules are created to configure Server or Domain Isolation rules that blanketly require IPSec negotiation to access network resources. Once configured, Isolation policies can require a combination of user and computer (endpoint) authentication using a combination of Kerberosv5 and certificates.
- **Authentication Exemption** These policies are used to configure exemptions to isolation policies configured in the environment. They can be tied to predefined computer types, IP addresses, ranges of IP addresses, or even whole subnets.
- **Server-to-Server** These policies apply Connection Security Rules to specific endpoints, creating a tunnel between the two hosts any time they exchange traffic.
- **Tunnel** When Windows Servers are being used as gateway devices routing traffic between subnets or disparate networks, the system administrator can use a tunnel Connection Security Rule to specify IPSec requirements for the traffic. This can be especially useful for circumstances where this traffic must pass across the public Internet. These types of connections are also called static VPNs.
- **Custom** When one of the default connection security scenarios doesn't exactly match the business requirements, the network administrator can build a custom rule to establish appropriate connection controls.

EXAM WARNING

Building a connection between two machines requires more than just a Connection Security Rule. The rule only establishes the requirements that must be met for the connection to be established. Appropriate network routes with Inbound and Outbound firewall rules must also be made to let network traffic flow.

Firewall Rules

Within the Windows Firewall with Advanced Security, a network administrator can configure individual firewall rules to control the flow of network traffic to and from the server. These are defined as both inbound (ingress) and Outbound (egress) rules that inspect traffic at the network level before they cross the boundary

between the network and the attached computer. This protects the computer from having to deal with inappropriate traffic and stops prohibited traffic from even leaving the workstation.

EXAM WARNING

For a single Protocol or application, it is possible to have different inbound and outbound firewall rules. It is important to understand that just because communication can be initiated in one direction, doesn't mean it can be established in the opposite one.

By default, a number of different rules are automatically created to provide a baseline of security before any manual configuration can take place. Not all of these rules are activated by default, but will be effected depending upon the server roles and options configured. In addition to these, the network administrator can create new rules to control traffic, such as:

- **Program Rules** These rules apply to connections associated with running specific applications and allow that specific program to accept inbound connections or initiate outbound connections. Program rules will often have to be created for applications that work in a client-server mode like antivirus, monitoring, or even business applications. This kind of firewall rule can be especially useful if the port that an application uses is not fixed.
- **Port Rules** When you specifically know what ports you need to control within the TCP/IP stack, you can explicitly specify them in a Port Rule. Many common applications will have “well-known” ports that they use to pass network traffic, or specific ports might be listed in product documentation.
- **Predefined Rules** Windows Server 2008 provides many different services to support network operations and system roles. These will often have complicated profiles using different types of connections across several ports. These predefined rules batch the network footprint of these Windows services making firewall configuration easier and reducing the time required to implement secure network communication.
- **Custom Rules** In the event that one of the built-in options in this list don't suit your network requirements, the Windows firewall lets you build your own rules to match applications and network communications to your exact needs.



TEST DAY TIPS

Windows Firewall with Advanced Security was first introduced in Windows Vista and was further refined in Windows Server 2008. While system firewalls have been available in the previous products, these cannot provide the comprehensive policy-based control available in the current platform.

Server and Domain Isolation

Both Server and Domain Isolation are network design methodologies that draw heavily on the network access technologies available in the Windows Server platform and are enhanced by the new technologies available in the Server 2008 product. The introduction of NAP, new VPN technologies, enhanced support for 802.1x, and better control of clients through Group Policy Objects (GPOs) have converged to bring new strength to the existing isolation strategies, adding a powerful tool to the network administrator's arsenal.



TEST DAY TIPS

Server and Domain Isolation are not server roles or technologies that are new to the Windows Server 2008 platform. Rather, it is a methodology that draws on the strengths of the core server technologies to provide a robust security infrastructure without having to make a significant investment in new technology.

Server and Domain Isolation allows the network administrator to leverage existing investments in network infrastructure and server hardware to provide a logical structure to protect data and segment access rather than having to make significant investments to implement complicated physical architectures. This lets user authentication and network policies that are already in place better manage security and

data access rather than force the administrator to introduce additional complexity or tools that would require new training.

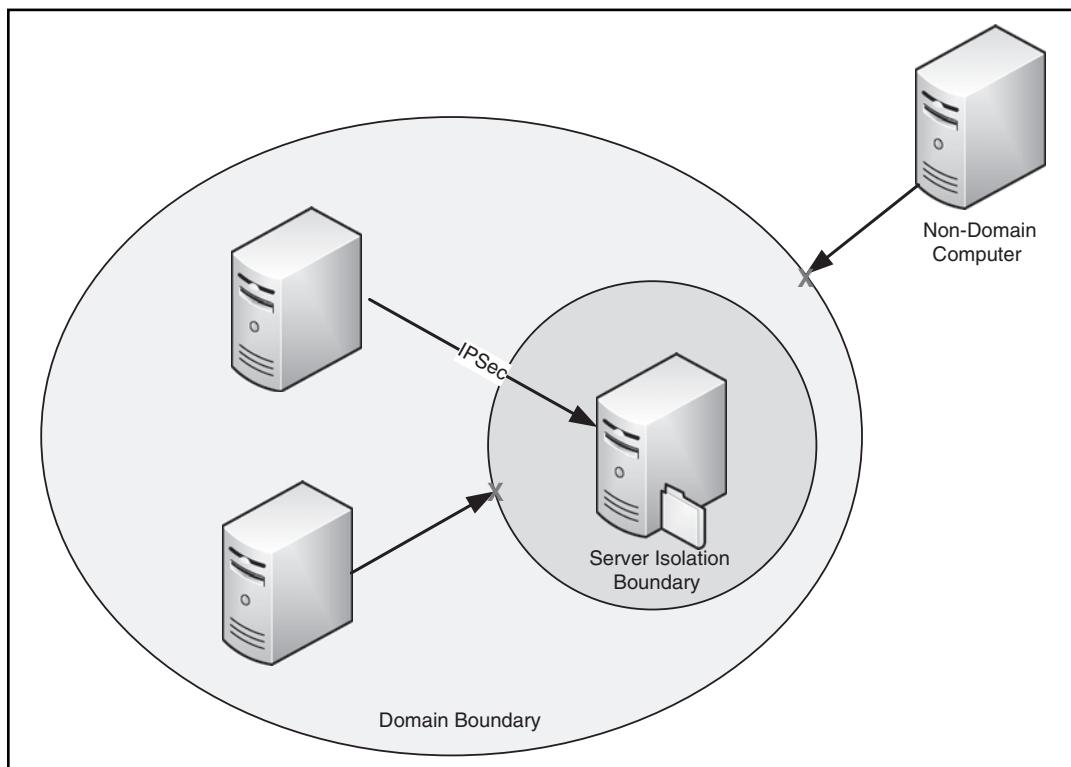
Using Group Policy and IPSec for tunneling and encryption, the network administrator can implement additional security checks and provide comprehensive access control to support compliance and auditing requirements. Important corporate data can be encrypted and access methods controlled through policies and NAP to ensure data integrity while improving availability.

One of the core benefits of either isolation strategy is that it more tightly ties access to domain resources to domain membership. Without any isolation in place, it is tempting to implement *ad hoc* changes to network permissions, allowing external users or inappropriate machines to access network resources. Even though these changes are meant to be temporary, they often don't get removed and, over time, result in security holes and backdoors into your systems. Implementing isolation requires domain membership and can help curb unplanned changes.

Benefits of Server Isolation

Corporate networks provide a diverse landscape of data and resources that all might have different security and access requirements. A server that is hosting common shared directories that are accessible to all employees will have a dramatically different security profile than a server that is used to house payroll or human resources data. More than just file permissions, these servers may have different requirements for security of access, access method, or even encryption of data in transit. This is well beyond the scope of what file and share permissions are able to do.

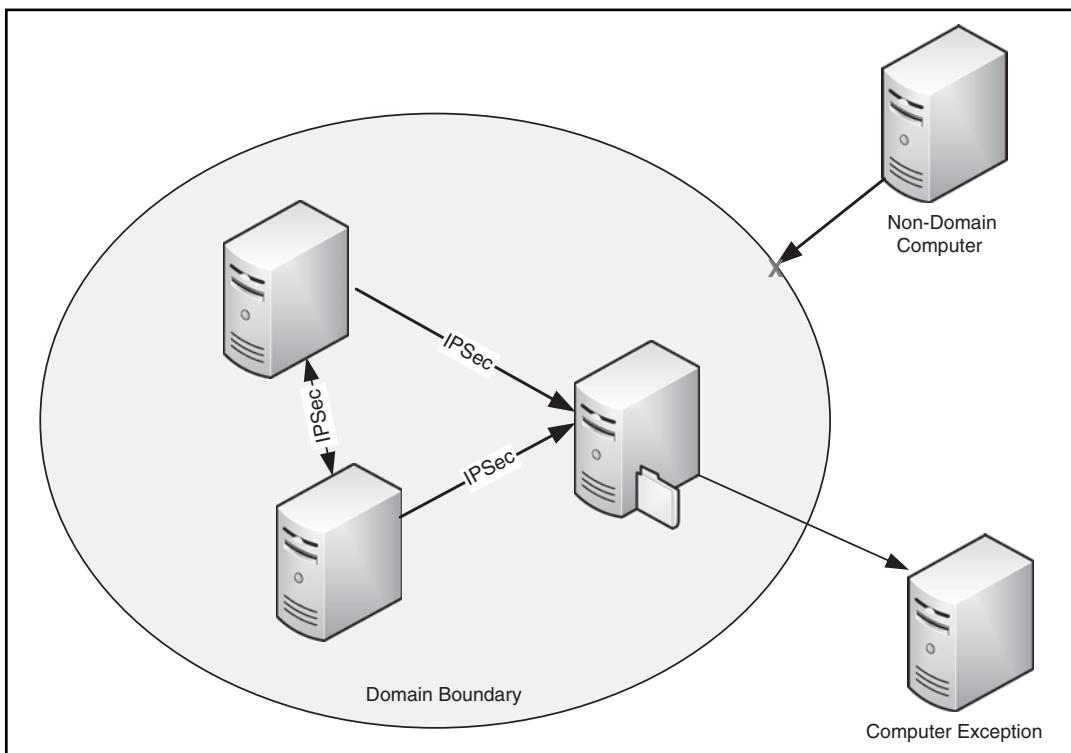
More than just resource access, simple permissions cannot protect servers from other network-based threats originating from workstations or devices outside of the domain. Without a server isolation policy (see Figure 2.30), viruses and spyware can flood the network, potentially causing a Denial-of-Service attack, or allow an attacker to intercept sensitive data en route.

Figure 2.30 Server Isolation

Benefits of Domain Isolation

Domain Isolation provides a broader scope of control than other isolation methods. Rather than focusing on specific server targets for isolation, all domain traffic between peers is governed by policies that can enforce authentication and encryption requirements on the traffic. This ensures that only authenticated domain partners are able to send or receive traffic on the network, requiring domain membership for participation.

Domain isolation is ideal for high-security applications or networks that carry a high level of risk because of public access or security holes. The use of IPSec tunnels between domain peers can protect against data sniffing, host spoofing, or even more advanced Man-in-the-Middle attacks (see Figure 2.31).

Figure 2.31 Domain Isolation

Developing an Isolation Strategy

Neither isolation strategy is mutually exclusive, as both are often deployed in the same environment providing overall domain coverage between domain peers and specific group-based control for sensitive systems. It is important that you have a well-defined set of requirements so your planning and testing can be kept to that scope. It is easy to want to implement domain and server isolation too quickly, resulting in resource unavailability and additional work-mitigating problems.

A good isolation strategy might consist of the following:

- **Clearly Define Goals and Expectations** Setting a goal to use server isolation to protect access to a payroll server is much different than a broad plan to isolate all accounting traffic on the network. Having clear objectives helps you measure success and will allow the project to be carefully executed in steps.
- **Understand Your Network Topology** It is important to have a clear understanding of your network, how it is configured, and how physical devices are related to overall business function. Implementing a server isolation strategy to restrict human resources data might be a good idea, but if the server also shares its function with other departments, the impact would be wider than anticipated.
- **Test in a Lab Environment** Changes to IPSec policies in the domain can impact everything from client communication to Active Directory replication. It is usually a good idea to test your implementation plan in a physically isolated environment that is not connected to your corporate network.
- **Implement Gradually** Domain and Server Isolation are controlled centrally through group policies. This means that the scope of deployment can be controlled through the use of OUs and GPO filtering. You can designate a small pilot group as your first wave of the deployment and grow that until the project is complete. This also allows for a quick backout should a problem arise in the implementation that must be corrected before moving on.

EXAM WARNING

Server Isolation is specifically concerned with controlling traffic between a client and a server resource, whereas Domain Isolation is a more widely scoped policy controlling traffic between domain peers as a whole.

Summary of Exam Objectives

Implementing an effective network access strategy is a broad goal that will draw on almost all parts of the server operating system to build a single unified plan. The Server 2008 platform provides many new and powerful tools that can be used to control network access like never before, allowing a true user-centric view of the network operations. These tools can provide reliable and secure access to corporate data to the end user any time, any place, and on almost any device.

When developing a strategy that will be effective and that will achieve corporate buy-in, it is important to lead from the business objectives rather than from the technology. Technology that is implemented for its own sake is doomed to fail and will only incite users to come up with their own workarounds to circumvent the planning you have done. It is when these technologies work behind the scenes, enabling business users, that they become the most useful, balancing the need for ubiquitous access with sound implementations of Authentication, Authorization, and Accounting.

To accomplish this, Microsoft has introduced NPS, which allows business rules to be created to validate the health criteria that must be met for workstations and other devices to participate on the network. This means that computers that don't meet the minimum requirements for systems such as antivirus, system patching, anti-spyware, and the like will be prevented from accessing corporate systems, protecting them from outside attack. This extends well beyond just workstation connections, too. These NAP policies can be evaluated and enforced across a variety of access methods, including wireless access, VPN connections, Terminal Services connections, and DHCP requests.

New types of externally originated connections are also introduced in Server 2008, as well as VPN technologies that have been expanded to include the SSTP protocol to support VPN tunneling through HTTPS. Terminal Services has also gotten an overhaul, introducing a number of new access services that provide Web client access, server load balancing, RemoteApp programs, Web gateways, and improved management.

Finally, the Windows Firewall has been improved and expanded to provide comprehensive access control and been integrated with IPSec tunneling to provide secure connections for your network, leading to improvements in both Server and Domain Isolation models.

Exam Objectives Fast Track

Network Access Policies

- NAP is a technology new to the Server 2008 platform to allow network administrators to control participation on the network based on the workstations' match to certain health criteria to minimize the risk to the overall network.
- System Health Agent (SHA)** This is a client-side application that is responsible for reporting on the health of a particular client subsystem when queried. This might be an agent or a service built into an existing application (for example, antivirus, updates, and so on).
- Statement of Health (SoH)** A Statement of Health is created to certify the client health at a particular moment in time.
- NAP Enforcement Clients (NAP EC)** This client application is responsible for enforcing the network access decision returned from the NAP system.
- System Health Validators (SHV)** This server component is responsible for the evaluation of individual SoH statements for the individual SHAs.
- NAP Enforcement Server (NAP ES)** This is the component responsible for comparing the overall health of the client machines against the access policies of the NAP system.
- Remediation servers provide services to clients on the network that are not compliant with the health policy for network access. These services allow the clients to bring themselves into compliance.

Remote Access Strategies

- All network access should be considered in the remote access strategy as the point of least security, and is the common denominator that determines the overall soundness of the network. RAS should be planned to allow access without introducing new risks to the corporate environment.

- Virtual private networks (VPNs) create secure client-to-network or network-to-network tunnels that traverse the public Internet. These are created to provide *ad hoc* network access or even more permanent WAN connections.
- To provide security for corporate data, an authentication method must be chosen to provide identification of the endpoints (PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP).
- Data encryption methods should also be chosen to ensure secure transfer across the VPN (PPTP, L2TP/ IPSec, SSTP).
- The Secure Socket Tunneling Protocol (SSTP) is a new offering to the Server 2008/ Vista environment, creating tunnels over standard SSL ports (TCP/ 443) allowing VPNs across firewalls with NAP integration.
- Terminal Services has been dramatically upgraded from previous versions, providing true enterprise-class terminal access.
- Terminal Services Session Broker** The session broker allows for Terminal servers to be aggregated into farms to provide highly available TS-enabled applications and desktop sessions. These can be load-balanced either in a round-robin scheme or based on load criteria.
- Terminal Services Gateway** Rather than opening terminal servers to the outside world, TS-Gateways can be deployed in the corporate perimeter network, allowing sessions to be initiated in a secure manner.
- Terminal Services Web Access** For users who may not have the full RDP client, terminal applications and desktop sessions can be enabled through the Web browser. This provides additional flexibility and allows applications to be run on a wider range of devices.
- Remote App** Rather than enabling a full desktop session, individual applications can be enabled through the terminal servers that will look and behave like local applications. This provides a much better user experience with all the benefits of a terminal environment.
- Corporate Desktop** Rather than exposing a server desktop to end users who may be unfamiliar with the server-class options, the Corporate Desktop simulates a Vista desktop that should be much more familiar to them and require less training to use.

Working with Perimeter Networks

- Perimeter networks are often called demilitarized zones (DMZs) that act as an intermediary between the public Internet and the internal corporate network.
- Most networking rules specify an implicit deny stratagem for perimeter networks, meaning that all traffic from a less-secure network to a more-secure network is denied, unless explicitly permitted by network rules.
- Network access from the Internet to the internal corporate network should almost always be avoided. All data and services for public consumption should be placed in the perimeter network.

Server and Domain Isolation

- It is often important to segment which clients should be able to securely communicate with different network assets across the corporation.
- Server Isolation uses SSL to allow specified groups of clients to access workgroup-specific server resources.
- Domain Isolation creates a strong domain policy, encrypting and signing domain traffic and requiring domain membership for secure resource access.

Exam Objectives

Frequently Asked Questions

Q: I would like to implement NAP to provide better protection of my network and require that workstations meet specific health criteria. How should I go about this?

A: It is important to fully test any NAP implementation before taking it fully into production. Many network administrators will choose to implement NAP in stages, rolling it out to only one access method at a time and breaking the user groups into smaller units, often completing implementation for a single department before moving on to the next. This gives you the opportunity to completely resolve any issues before moving on to a bigger group. You can also control the communication plan and organizational impact by dealing with smaller units or geographical areas one at a time.

Q: I would like to implement a Network Access Policy, but I am not able to upgrade all of my servers to Windows 2008 and my workstations to Vista. What options do I have to protect my network from unauthorized access and ensure the health of my workstations?

A: Not all of the servers on a network have to be upgraded to Windows Server 2008 to be able to support NAP. As long as the servers hosting the NAP infrastructure are running Server 2008, you will be able to implement access policies. In order to use the full functionality of NAP, you will need to update your workstations to Vista SP1 or Windows XP SP3.

Q: In my Windows Server 2003 environment, I am running Internet Authorization Service (IAS), but I don't see that as an option in Server 2008. What are my options and is there an upgrade path?

A: The IAS product has been brought into the core of NPAS, but how you migrate will largely depend on what you were using it for. Usually, network administrators use IAS to provide authentication of wireless access points and 802.1x authorization. In Server 2008, these have been broken out into more discrete units so you can better control them as policies. In this case, using the wizards will give you the best results. For more custom implementations or RADIUS proxy, you will still need to configure RADIUS directly.

Q: I am planning to configure firewall rules to allow specific ports into my servers. What are common ports that I should know when planning port access rules on my Windows Firewall with Advanced Security?

A: A number of ports fall under the heading “well-known ports,” of which a network administrator should be aware. While this is not an exhaustive list, these should at least be somewhat familiar:

| | |
|-------------------|--|
| TCP/20 & TCP/21 | These run the File Transfer Protocol (FTP) |
| TCP/23 | TELNET traffic |
| TCP/25 | Simple Mail Transfer Protocol (SMTP) for e-mail |
| TCP/53 | Domain Name Server (DNS) traffic |
| UDP/69 | Trivial File Transfer Protocol (TFTP) |
| TCP/80 | HyperText Transfer Protocol (HTTP) |
| TCP/88 & UDP/88 | Kerberosv5 traffic |
| TCP/110 | Post Office Protocol v3 (POP3) |
| UDP/123 | Network Time Protocol (NTP) |
| TCP/137 & UDP/137 | NETBIOS Name Service |
| UDP/138 | NETBIOS Datagram Service |
| TCP/139 | NETBIOS Session Service |
| UDP/161 | Simple Network Management Protocol (SNMP) |
| TCP/443 | Secure HTTP |
| TCP/1433 | MS SQL Communication |
| TCP/3389 | Remote Desktop Protocol (RDP – Terminal Services) |

Q: I am concerned about security and am trying to decide if using the Windows Server Core is right for me. For that matter, if it is so much more secure, why wouldn’t I use that as the default for all of my servers?

A: Implementing the Windows Server Core can dramatically increase security of a system if it is done properly and if careful planning is taken to ensure that only needed components are configured on your servers. The decision to implement is really a business decision. Implementing Server Core can introduce some risk to the environment since network administrators are not generally accustomed to making all changes at the command prompt and a lack of familiarity can lead to configuration mistakes. There is also a cost associated with the learning curve and a possible loss in reaction time—if you’re reacting to a specific threat

and can't get something done quickly because you have to look up commands, the business could be put in jeopardy.

So, before implementing server core, be sure that the use is appropriate, that you have staff who are able to support it well, and that you understand that the additional security comes at the cost of additional manpower to maintain it.

Self Test

1. You are implementing a Windows 2008 network that will rely on NAP to ensure that clients participating on the network always have updated antivirus definitions before they are able to participate on the network. When these clients log on, they will be required to request access to the network and assert their fitness to access domain resources. This process is an example of?
 - A. Authentication
 - B. Authorization
 - C. Access
 - D. Accounting
2. You are planning to implement a network access security plan that will use the Windows System Health Agent (WSHA) to issue workstations' SoH declarations to the NAP Server. You are concerned that some workstations will not be able to participate on the network after NAP has been enabled. Which operating systems will you have to upgrade?
 - A. Windows XP SP2
 - B. Windows Vista SP1
 - C. Windows Server 2008
 - D. Windows Server 2003 R2
3. You are planning to implement NAP on your network with a variety of Enforcement Clients (NAP EC) that will tie it to appropriate enforcement points. You are planning to use the 802.1x protocol as the authorization component of NAP to validate computer certificates for domain authentication. Which network access technologies can this solution control?
 - A. Terminal Services Connections
 - B. Wireless Communications
 - C. Wired Switch Port Access
 - D. IPSec Connections
 - E. VPN Connections

4. You are troubleshooting a workstation that is not able to participate on the network because the NAP Agent isn't functioning correctly. Which fundamental communication will not occur until you restore the function of the NAP Agent?
 - A. Creation of the Statement of Health declarations
 - B. Creation of the System Statement of Health
 - C. Validation of the NAP policies
 - D. Creation of the Statement of Health Response
5. The NAP Health Registration Authority must be able to communicate with a number of different resources on your network to function correctly. Which services must be installed for the NAP HRA to participate on the network?
 - A. Active Directory
 - B. DHCP
 - C. NAP Administration Server
 - D. Certificate Authority
6. You're planning to use the Windows System Health Agent (WSHA) as the primary SHA responsible for evaluating client health. You want to make sure that you have the appropriate resources available on the remediation network so workstations will be able to bring themselves into compliance. What resources might you want to make available to allow these machines to become compliant?
 - A. The domain controller
 - B. Windows Server Update Server (WSUS)
 - C. Install files for Antivirus
 - D. Certificate Authority
7. You are an administrator of a corporate network and would like to configure a reliable and consistent environment for a training lab that will be based on thin-client workstations rather than complete workstations. Because you will be doing different kinds of training in the lab, it is important that these thin clients are able to easily adapt to the changing needs of the trainers. What kind of Terminal Services implementation would give the training staff the most flexibility when using this lab?
 - A. Deploy a number of RemoteApp programs to match the training needs.
 - B. Enable Remote Desktop for Administration.

- C. Configure Terminal Services Web Access.
 - D. Configure Terminal Services with Vista Desktop.
8. For the several months you have been running a network application over Terminal Services, it has become a core part of your business. Now that this application is considered to be mission-critical, what next steps should you take to ensure it is always available to the enterprise?
- A. Implement RemoteApp to ensure the application is secure and to increase the stability of the server by isolating the application from the operating system.
 - B. Implement Session Broker and deploy additional terminal servers to provide a server farm with load balancing.
 - C. Implement Terminal Services Gateway to make the application available to the outside world and bring it into the scope of the corporate NAP authorization.
 - D. Implement Terminal Services Web Access to make the application available to remote users who may not have access to the RDP Client.
9. Your terminal servers have suddenly stopped providing terminal connections to non-administrator clients trying to open terminal connections. What is the first thing you should check?
- A. Check to be sure that the Terminal Services Licensing Service is running.
 - B. Ensure that the terminal server is running.
 - C. Restart the TS Broker Service.
 - D. Restart IIS to reset TS Web Access.
10. Your company is planning to deploy a sales management system and would like to make this available to its traveling sales force as they move from client to client. You are planning to implement Terminal Services Client Access Licenses (TS CALs) in per-device mode. What is the downside of this choice?
- A. The sales force will not be able to access the terminal server remotely.
 - B. Traveling agents will only be able to connect from corporate laptops.
 - C. The number of licenses purchased will have to match the number of remote sales agents.
 - D. You will not be able to load-balance connections through the TS Broker Service.

Self Test Quick Answer Key

- | | |
|----------------|-------------------|
| 1. B | 6. B, C, D |
| 2. A, D | 7. D |
| 3. B, C | 8. B |
| 4. B | 9. A |
| 5. C, D | 10. B, C |

Chapter 3

MCITP Exam 647

Active Directory Forests and Domains

Exam objectives in this chapter:

- Designing Active Directory Forests and Domains
- Designing Active Directory Topology
- Designing Active Directory Administrative Model

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

There has been a lot of hype about Windows Server 2008 Active Directory Domain Services (AD DS). There have been many changes since the days of Windows 2000's Active Directory. Some of the aspects of AD DS that have changed significantly include auditing, fine-grained password policies, read-only domain controllers, Restartable Active Directory, Database Mounting Tool, and user interface (UI) improvements. Even though this chapter concentrates on the design of Active Directory, having an understanding of the changes will benefit you as well.

In this chapter you will learn about some of the advances in domain services. You will also learn about designing forests and domains, implementing those functional groups by designing your network topology, and finally, how to administer your network effectively by designing an administrative model.

New in Windows Server 2008 Active Directory Domain Services

In Windows 2000 Server and Windows Server 2003 Active Directory, there was only one audit policy, **Audit Directory Service Access**, that controlled whether auditing for directory service related events was enabled or disabled. In Windows Server 2008 Active Directory, this one policy is further subdivided into four subcategories:

- Directory Service Access
- Directory Service Changes
- Directory Service Replication
- Detailed Directory Service Replication

Windows Server 2008 has added the capability of auditing old and new values of an attribute when a change has been successfully committed to the database. Previously, Directory Service Access only logged the name of the attribute that was changed; it did not log the old and new values.

The ability to audit changes to objects in AD DS is enabled with the new subcategory **Directory Service Changes**. The types of changes that you can audit are create, modify (except for delete), and move and undelete operations performed on an object. Each of these events will appear in the security log in the Event Viewer. This new policy subcategory adds the following capabilities to auditing in AD DS:

- **Create** Upon the successful creation of an object, the attributes that are populated during the create operation get logged. In some cases, AD DS

will assign a default value, such as sAMAccountName; these attributes do not get logged.

- **Modify** If successful, AD DS logs the previous and current values of the attribute. If the attribute has more than one value, only the attribute value that changed gets logged.
- **Move** If an object is moved within a domain, AD DS logs this like a modify event; that is, it will log the previous and current values of the distinguished name (DN). If an object is moved to a different domain, then create will be logged on the target AD DS domain controller.
- **Undelete** Upon the successful undelete of an object (authoritative restore), the location to which the object was moved to gets logged. If attributes get modified (added, removed, or changed) during the undelete, then those modified attributes get logged.



TEST DAY TIP

When an object is deleted, Directory Service Change does not log the event. Instead, an event gets logged by Directory Service Access.

In previous versions of Windows, all the way back to Windows NT, if you had different groups of users with either different password requirements, or different lock-out policies, Windows required you to put these users into different domains. This is because password policies were set at the domain level. This made managing these users less efficient, as you really had two choices: either give everyone the same password policy which was too secure for some but not secure enough for others, or create several domains. In Windows Server 2008 AD DS, you can create different password and lockout policies based on AD security groups.

Fine-grained password policies allow you to specify multiple password policies within a single domain. The fine-grained password policies can apply different password and lockout policies to different sets of users within a single domain. The policies, however, only apply to user objects and global security groups, and only members of the Domain Admins group can apply fine-grained password policies. You can, however, delegate permissions to other trusted users or groups of users to set these policies. Also the domain function level must be set to Windows Server 2008.

You use the MMC snap-in ADSIEDIT to create and apply fine-grained password policies. The following password and lockout settings can be applied using these policies:

- **Enforce password history** How many passwords changes are stored and cannot be repeated
- **Maximum password age** Maximum number of days your password can be kept before it is required to be changed
- **Minimum password age** Minimum number of days you must have your password before you are allowed to change it again
- **Minimum password length** Minimum number of characters your password must contain
- **Passwords must meet complexity requirements** Determines if your password must contain a combination of upper and lower-case letters, numbers, and special characters and be a certain minimum length.
- **Store passwords using reversible encryption** This security setting provides support for protocols that must know the users password for authentication purposes. The Remote Access Protocol CHAP (challenge hand-shake authentication protocol), for example.
- **Account lockout duration** If your account is locked out due to a certain number of invalid log on attempts, this settings specifies how long it will be locked out for.
- **Account lockout threshold** This setting specifies how many bad logon attempts, or invalid password entries, will be allowed before your account must be unlocked.
- **Reset account lockout after** This setting specifies how many minutes the domain controller should wait before resetting the count of bad logon attempts. For example, if this setting is set to 30 minutes, and the Account lockout threshold is 5, with every bad logon attempt, the domain controller is keeping tally so that your account can get locked out. If after 4 bad password entries, you decide to wait 30 minutes, the domain controller will clear your tally of bad logon attempts so you can have 5 more chances.



NOTE

All of these attributes have a **must have** attribute, this means that each of these values must be set. Also, settings from multiple password policies cannot be merged.

EXERCISE 3.1

CREATING AND APPLYING FINE-GRAINED PASSWORD POLICIES

1. Click Start | Run, type **adsiedit.msc** and then press **Enter**.
2. In the **ADSI Edit** snap-in, from the **Action** menu click **Connect to...**
3. Accept the **Default naming context** and then click **OK**.
4. Double-click the **Default naming context** and then expand the **Domain**.
5. Expand **CN=System** and then click **CN=Password Settings Container**.
6. In the **Actions** pane click **New | Object**.
7. In the **Create Object** dialog box, click **Next**.
8. On the **Common-Name** page, in the **Value** field, type a name for this password settings object (PSO), and then click **Next**.
9. On the **Password Settings Precedence** page, in the **Value** field type a number greater than 0 and then click **Next**. (If a user has more than one PSO because of different security group memberships, the PSO with the lowest value here wins.)
10. On the **Password reversible encryption status for user accounts** page, in the **Value** field type either **FALSE \ TRUE**. (**FALSE** is recommended.)
11. On the **Password History Length for user accounts** page, in the **Value** field type a number between 0 and 1024.
12. On the **Password complexity status for user accounts** page, in the **Value** field type either **FALSE \ TRUE**. (**TRUE** is recommended.)
13. On the **Minimum Password Length for user accounts** page, in the **Value** field, in the **Value** field type a number between 0 and 1024.
14. On the **Minimum Password Age for user accounts** page, in the **Value** field type a value using the **I8 format**. (For this exercise type **-864000000000** or the I8 value of one day.)
15. On the **Maximum Password Age for user accounts** page, in the **Value** field type **-3628800000000** or the I8 format value of 42 days.
16. On the **Lockout threshold for user accounts** page, in the **Value** field type **-0** or the I8 format for do not lockout user accounts.

17. On the **Observation Window for lockout of user accounts** page, in the **Value** field type **-180000000000** or the I8 format value of 6 minutes.
18. On the **lockout duration for locked out user accounts** page, in the **Value** field type **-180000000000** or the I8 format value for 30 minutes.
19. On the **To set more attributes**, click **More Attributes** page.
20. In the **cn=PSO Name** dialog box, in the **Select a property to view** drop-down window select **msDS-PSOAppliesTo**. In the **Edit Attribute** field, type the distinguished name (DN) of the security group to apply this PSO to; then click **Add** and **OK**.
21. Click **Finish**.



NOTE

For help in understanding the I8 format, visit:

<http://technet2.microsoft.com/windowsserver2008/en/library/4855d7f6-0e70-4de3-a892-052c81c50f7d1033.mspx?mfr=true>



TEST DAY TIP

Fine-grained password policies are a new feature of Windows Server 2008, and they will affect the way you design your Active Directory infrastructure. Therefore, you will most likely see questions regarding password policies.

With a read-only domain controller (RODC), you can easily deploy a domain controller in a location where physical security cannot be guaranteed. An RODC hosts read-only partitions of the AD DS database. RODC addresses some of the problems that are commonly found in branch offices. These locations might not have a domain controller. Or, they might have a writable domain controller but not the physical security, network bandwidth, or local expertise to support it. The following RODC functionality mitigates these problems:

- **Read-only AD DS database** The RODC holds the objects and attributes that a writeable domain controller holds, except for account passwords.
- **Unidirectional replication** Because the database is read only, changes cannot originate from the RODC.
- **Credential caching** By default, the RODC does not store user credentials. You must explicitly specify which users, if any, you wish to cache on the RODC.
- **Administrator role separation** Domain controllers do not have local administrators. However, on the RODC, because it is designed for branch offices with few users and no IT staff, a user at the branch office can be granted local administrator rights on the RODC without granting the user Domain Admin rights.
- **Read-only Domain Name System (DNS)** The DNS server can still hold application partitions and other directory partitions for users to use when querying for servers and services. However, the read-only DNS server does not support client updates, and any client wishing to update their A record, would get redirected to a writeable DNS server to perform the operation.

Restartable Active Directory reduces the amount of time it takes to do certain administrative tasks. In previous versions of Active Directory, if you wanted to perform an offline defragmentation of the directory database, you had to shut down the domain controller and restart in Directory Services Restore Mode (DSRM). When this happened, users would get disconnected from the domain controller and, if the server were also hosting DFS or DHCP, users would not be able to connect until it was rested again normally.

Now to stop the AD DS service, you simply go into the Services.msc, Computer Management, or the Services (local) node in Component Services. Then click the service, and then click **Stop**. When you have completed your task, simply start the service again.

The Active Directory database mounting tool allows you to compare data as it exists in snapshots, or backups, that are taken at different times so you can better decide what data to restore after data loss. This is more efficient than restoring from multiple locations to find the data that you need. Please note, however, that the mounting tool does not actually recover any data; but it makes it easier to compare the data prior to your recovery efforts.

The Database Mounting Tool works with Volume Shadow Copy Service (VSS) to take snapshots of Active Directory, without the need to stop the AD DS service.

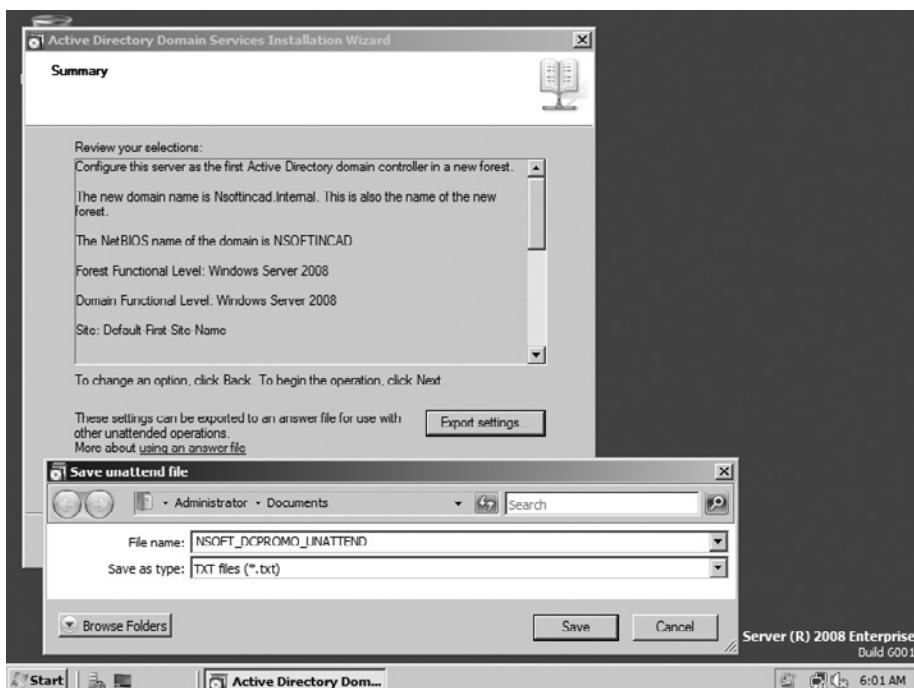
NOTE

Although it is not required, it is a good practice to use Task Scheduler to run Ntdsutil to take snapshots of the volume that is holding the directory database.

AD DS UI improvements provide new installation options for domain controllers. Also, the updated Active Directory Domain Services Installation Wizard streamlines and simplifies AD DS installation. Some of the new UI features of the installation wizard are:

- Uses the credential of the logged on user, or you can specify different credentials if necessary
- You can create an answer file on the **Summary** page of the wizard, which can then be used as a template for additional DC installations. See the steps on page 19 on how to install Active Directory and create an answer file. See also Figure 3.1.

Figure 3.1 DCPromo Creating Unattend File



- You can omit the administrator account password from the answer file so that the user installing the DC will get prompted to supply one.
- You can force the demotion of a DC that is started in DSRM.
- When you are creating an additional DC in a child domain, the wizard will detect if the infrastructure master role is hosted on a global catalog (GC) and prompt you to transfer the infrastructure master role to the DC you are creating.
- You can pre-populate the wizard by launching it from a command line specifying several new parameters.
- The Active Directory Sites and Services MMC snap-in now includes a Find command, helping you to find in which site a domain controller has been placed.

Designing Active Directory Forests and Domains

Creating a forest design first involves identifying the groups within your organization that have the resources available to host the Active Directory forest. Second, you will need to identify your design requirements. Finally, you will need to determine the number of forests that your organization will require to meet your organization's needs.

Once the forest design is in place, it is up to the enterprise administrator to develop a domain design. That is, how many domains are necessary, what domain names will be used, will you be upgrading existing domains to Windows Server 2008 or creating new domains, and will you be consolidating existing domains to a smaller number of more efficient Windows Server 2008 domains?

Factors to Consider When Creating Forest Design Plans

Several factors need to be considered when creating your forest design plans. These factors will need to be considered whether creating a design for the first time or upgrading an existing forest, and whether you are designing a forest for a large, enterprise organization, or a small-to-medium-sized corporation. These factors include:

Business Units

Many organizations are actually made up of several smaller business units, which may or may not share some of the same IT infrastructure. Some of these business units may require isolation from the rest of the organization. If that is the case,

then a separate Active Directory forest may be required. In other cases, a single forest with distinct domains might be the answer. If your business units will share an IT infrastructure, it is best to put them into the same Active Directory forest. However, using separate domains may be required depending on the amount of security each business unit is requiring.

Schema

Some of your business units may require a schema modification that the rest of the organization does not need. Or an application, such as Microsoft Exchange Server 2007 or System Center Configuration Manager (SCCM) might get installed that will require a schema modification. Since the Active Directory forest is made up of a single schema, any business unit requiring a different, or modified schema, will need to be in its own isolated forest.

SCCM adds attributes to Active Directory. For example, the SCCM clients will browse Active Directory to find a management point in the same AD site as the client is in. For Active Directory to find the management point, an attribute gets added to the Active Directory schema, and a container gets added into Active Directory users and computers. If a portion of your organization will not be using SCCM and wishes to not have these schema modifications, that portion will have to be isolated into its own forest.

Legal

For legal reasons, you may need to isolate one business unit from other business units. This is common in financial institutions where there are certain regulatory bodies in place with distinct rules on data sharing between parts of the company.

Security

Large organizations will find that they require an isolated forest to protect their data from other business units. This is common practice in hosted environments as well as in financial institutions.

Namespaces

Each forest within an organization will have at least one unique DNS (domain name system) namespace; if there are multiple trees in the forest, there could be several namespaces within the organization. Each DNS namespace and the corresponding NetBIOS namespace must be unique across the entire enterprise. For more information on DNS in the enterprise, please see Chapter 1, Name Resolution and IP Addressing.



TEST DAY TIP

Windows Server 2008 DNS includes a new zone, called the GlobalNames Zone, which will eliminate the need to implement WINS (Windows Internet Name Service) in your organization. The GlobalNames Zone is discussed more in Chapter 1.

Timelines

A carefully planned Active Directory environment will not happen overnight, and the planning should not be rushed to simply stay within agreed upon timelines, especially if multiple business units are involved in the planning.

As we have already discussed, different business units in your organization may have different needs as it comes to implementing Active Directory. They also may have a different deadline in mind as it comes to designing and implementing Active Directory. It is possible that one business unit may be under a tighter timeline, as they require Active Directory to deploy Exchange Server, or some other directory-enabled application. However, if one business unit requires Active Directory deployment faster than another unit, it is possible that they will decide to forego the “shared” design of a single forest and deploy their own forest.

However, that doesn’t mean that when the other business units are ready they cannot join the now already existing Active Directory infrastructure; but planning the forest will have to take place if that will be the ultimate decision. Creating an isolated forest simply because all units cannot agree on a timeline should not be the practice, but the exception, and should be done only as a last resort.

Administrative Overhead

As we will learn, there are different designs that can be implemented. The most cost-effective, easiest-to-implement design would involve a single domain in a single forest, with a single administrative group. However, this model will not suit all businesses or even all business units in an enterprise-wide organization. A multi-domain, multi-forest design will typically require more administrators, a greater namespace, more hardware, extra money, and so on. However, carefully planning your group policy objects (GPOs) and other administrative functions can minimize the amount of administrative overhead. See Chapter 4 for more information on GPO design.

Many business units do require isolation, however; so consider how much isolation is required. For example, it is possible to use a single forest, but still maintain isolated

namespaces, and give administrative control of each domain to a different group of administrators. The enterprise administrator in the forest root domain will still have over-all control of the forest, but each domain administrator can control his own resources. Using an empty forest root is common practice when each domain must be managed separately. An empty forest root domain means that the forest root is created and holds the forest-wide operations master domain controllers, and holds the Enterprise Admins and Schema Admins security groups, but all other user and group accounts, as well as other objects, are created in their respective domains, and administrative control of each domain is given to the Domain Admins group in each domain.

Testing Environments

Before implementing Active Directory, each organization should create a testing environment that very closely mirrors that of the real deal. For example, in this test environment you should have domain controllers, DNS servers, exchange servers, OUs, group policies, etc. This test environment should remain isolated from the actual network, however, to ensure that no users gain administrative access over your real network inadvertently. During the planning and testing phases, it is important to test all applications for full functionality, and get the results signed-off by each business unit.

While creating this test environment consider that you will need extra hardware, and should try to create the same type of environment; that is, the same number of users and policies, the same type of network bandwidth, same number of sites, etc. It is common to use virtualization strategies, such as Microsoft Virtual Server 2005, to create your testing and production environments while minimizing your hardware costs. Windows Server 2008 also will have virtualization capabilities using Hyper-V. After your design and implementation is complete, consider keeping this environment for testing any new technology before adding it to the production environment.

Creating a Design Plan

Creating the design plan includes identifying those responsible for creating the design, which parts of the organization will be affected by the design, what hardware will be used, and so on. Members of this team should include your enterprise administrators, network and mail administrators, and others with knowledge of Active Directory and the users' needs. It is important to document every stage in the design, and document all important project deadlines. You should also have a plan on which to fall back in case something catastrophic occurs during the implementation phase.

When problems occur, you can rely on this documented plan, and each member of the team will already have steps to follow to revert back to the existing environment. This may include creating a backup of the existing Active Directory infrastructure, and documenting all of the servers in your organization, and what operations master roles each hold, if any.

Creating the correct design will make the conversion or upgrade to Windows Server 2008 a much better experience than going in blindly without a well-documented plan. As discussed in the following sections, there are many different elements to a good design. In addition to knowing how Active Directory can be used, the enterprise administrator needs to make decisions about how many domains and forests are necessary based on many factors, including network bandwidth, security, and the number of servers available. Figures 3.2 and 3.3 show the high-level processes in creating the forest and domain designs.

Figure 3.2 The Basic Steps in Creating a Forest Design

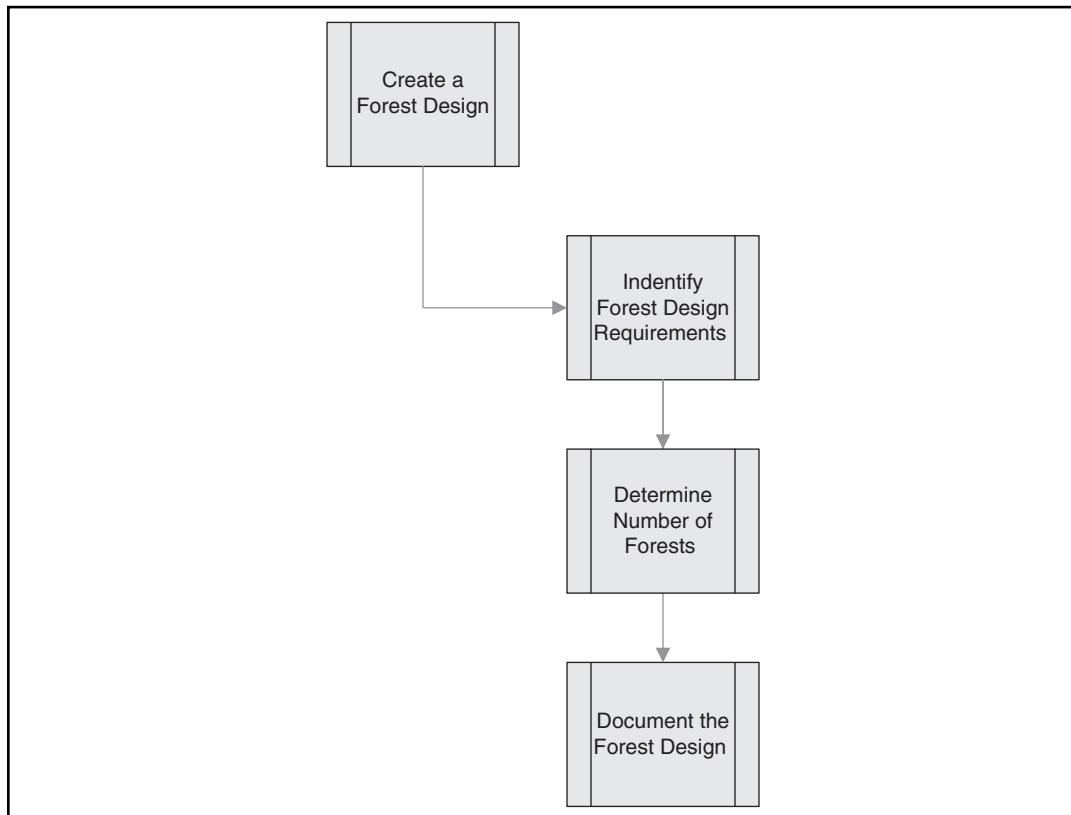
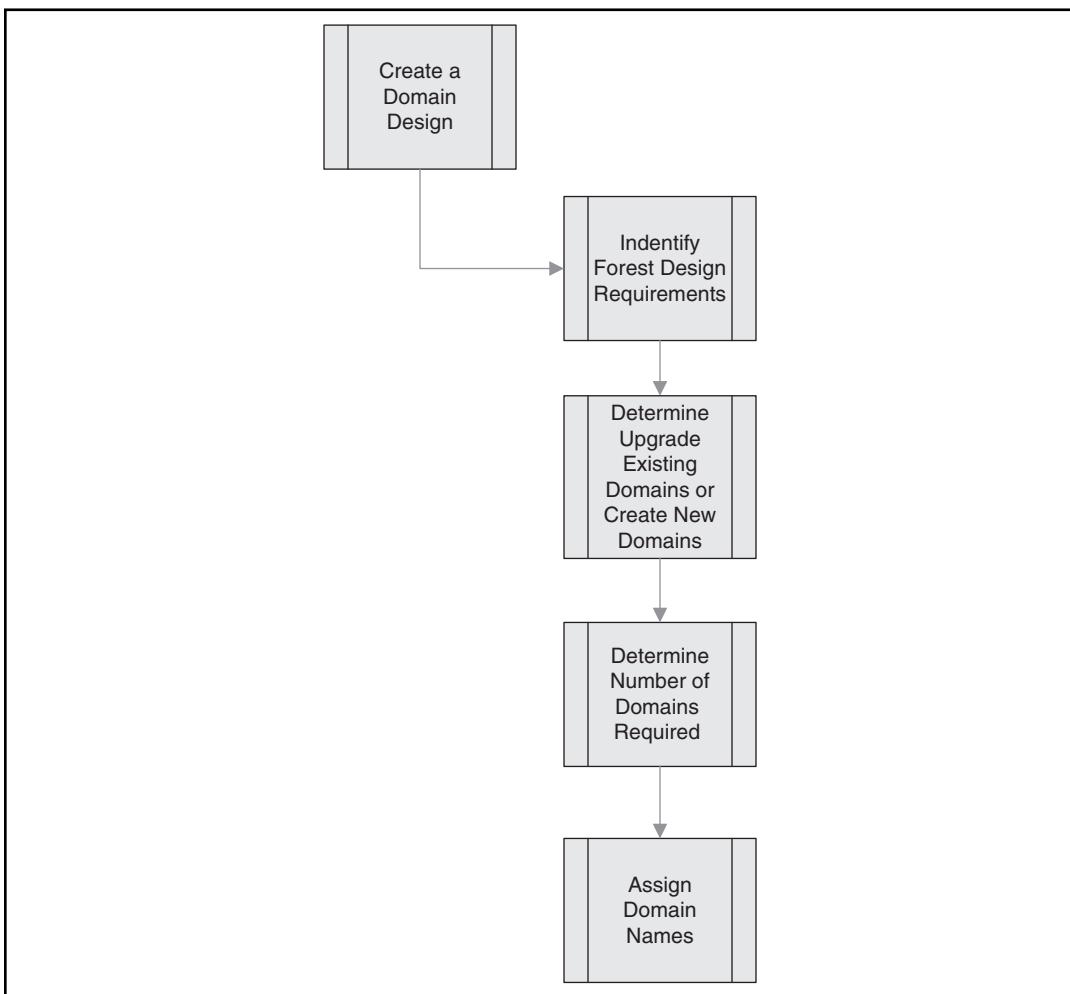


Figure 3.3 The Basic Steps in Creating a Domain Design**NOTE**

While the information included here about the steps necessary to design your forest and domains is useful, do not expect exam questions dealing with detailed information about these steps. Instead, remember that the number and names of forests and domains are not constant, and that the organization's specific requirements will determine this. Properly interviewing each member of the design team will help in determining these factors.

The Forest Structure

In Active Directory Domain Services (AD DS), the design can be broken into two distinct areas: The logical design, which is the design of the forest, domains, and OUs, and the physical design, which consists of the actual hardware that will be hosting AD DS and the physical location of these servers (AD Sites), and the links that allow for efficient routing of query and replication traffic, known as site links.

The Active Directory Domain Services (AD DS) Logical Design Structure

When you design an Active Directory logical structure before deploying AD DS, you can optimize your deployment process to best take advantage of Windows Server 2008 Active Directory features. Some factors to consider as you create your design include:

- Where to place the forest and domain boundaries
- How to configure the DNS environment for the forest
- How to design the organizational units (OUs)

Active Directory Domain Services (AD DS) in Windows Server 2008 allows organizations to create a secure, more scalable and more manageable infrastructure for user, group, computer, and other resource management. It also enables organizations to support directory-enabled applications. A well-designed AD DS logical structure also provides the following benefits:

- Simplified management of Windows-based networks that contain a large number of objects
- Reduced administrative costs with a consolidated domain structure
- The ability to delegate administrative control over resources, such as user and group accounts, or entire organizational units (OUs)
- Reduced impact on network bandwidth
- Lower total cost of ownership (TCO)

A well-designed Active Directory logical structure makes it more efficient for deploying group policies, public key infrastructure (PKI), domain-based distributed file system (DFS), and will better integrate with other applications, such as Microsoft Exchange Server.

Designing the logical structure for Active Directory is defining the relationships between the many containers in your organization's directory. The relationships between the containers might be based on an administrative model, such as delegating authority to OUs or grouping objects to better control group policy software deployment, or an operational model, such as controlling replication traffic. Even though traditionally we think of Active Directory Sites when we think of controlling replication traffic, the logical design has a big impact on this as well. In the following section we will get more into that.

The following elements make up the logical design: forests, trees, domains, and organizational units. Before you design the logical structure, it is important to understand the AD logical model. AD DS is a distributed database that stores information about network resources, and application-specific data from directory-enabled applications. AD DS allows administrators to organize elements of a network (such as users, groups, computers, and devices) into a hierarchical containment structure. On the top-level, the container is called the forest. Within forests are trees, within trees are domains, and within domains are OUs. This is called the logical model because it is doesn't matter in which OU a user account was created; they can still be authenticated by an AD DS domain controller in their own domain, or access resources on any server in any domain in the forest.

Active Directory Forest

As we have already discussed, the forest is the top-level container in any Active Directory environment. The forest is a collection of one or more Active Directory domains that share a common logical structure, directory schema (class and attribute definitions), directory configuration (site and replication information), and global catalog (forest-wide search capabilities). All domains in the same forest are automatically linked with two-way, transitive trust relationships, regardless of which tree in which they were created, which cannot be removed.

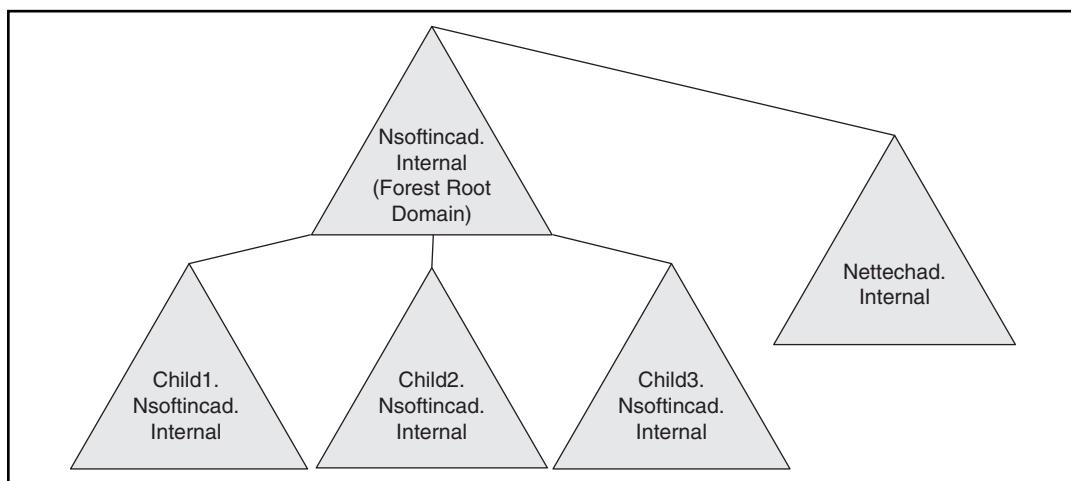
TEST DAY TIP

Because all domains in a forest share a single schema, if you have two business suits that require different schema objects to be enabled, you must put these domains into two different forests.

Active Directory Tree

The Active Directory tree enables you to assign completely different namespaces to different portions of your Active Directory forest. Because of the parent-child relationship between all domains in a tree, all child domains created take a portion of their parent domain's name. For example, a company called N-Soft, Inc., deploys Active Directory, and assigns the name Nsoftincad.Internal to the forest root domain. If tN-Soft also decides that it needs to create a child domain for each location within the forest, and use Nsoftincad.Internal as the parent domain, then the child domains will be called Child1.Nsoftincad.Internal, Child2.Nsoftincad.Internal, Child3.Nsoftincad.Internal, and Child4.Nsoftincad.Internal. However, if there is another business unit called WXYZ.com within the organization that does not need to use the ABCD namespace, then it can be created as a separate tree in the existing forest. In this way the transitive two-way trust relationship, single schema, global catalog, and so on, can be shared by all domains (see Figure 3.4).

Figure 3.4 Two Trees in a Forest. All Domains Share a Trust Relationship



Active Directory Domain

Previous versions of Windows (specifically Windows NT 4.0) defined the domain as a security boundary. That is, if the user account was not in this domain, and an explicit trust was not set up (in the right-direction), then the user had no access to any of the resources in this domain. In Active Directory, the domain became a partition in

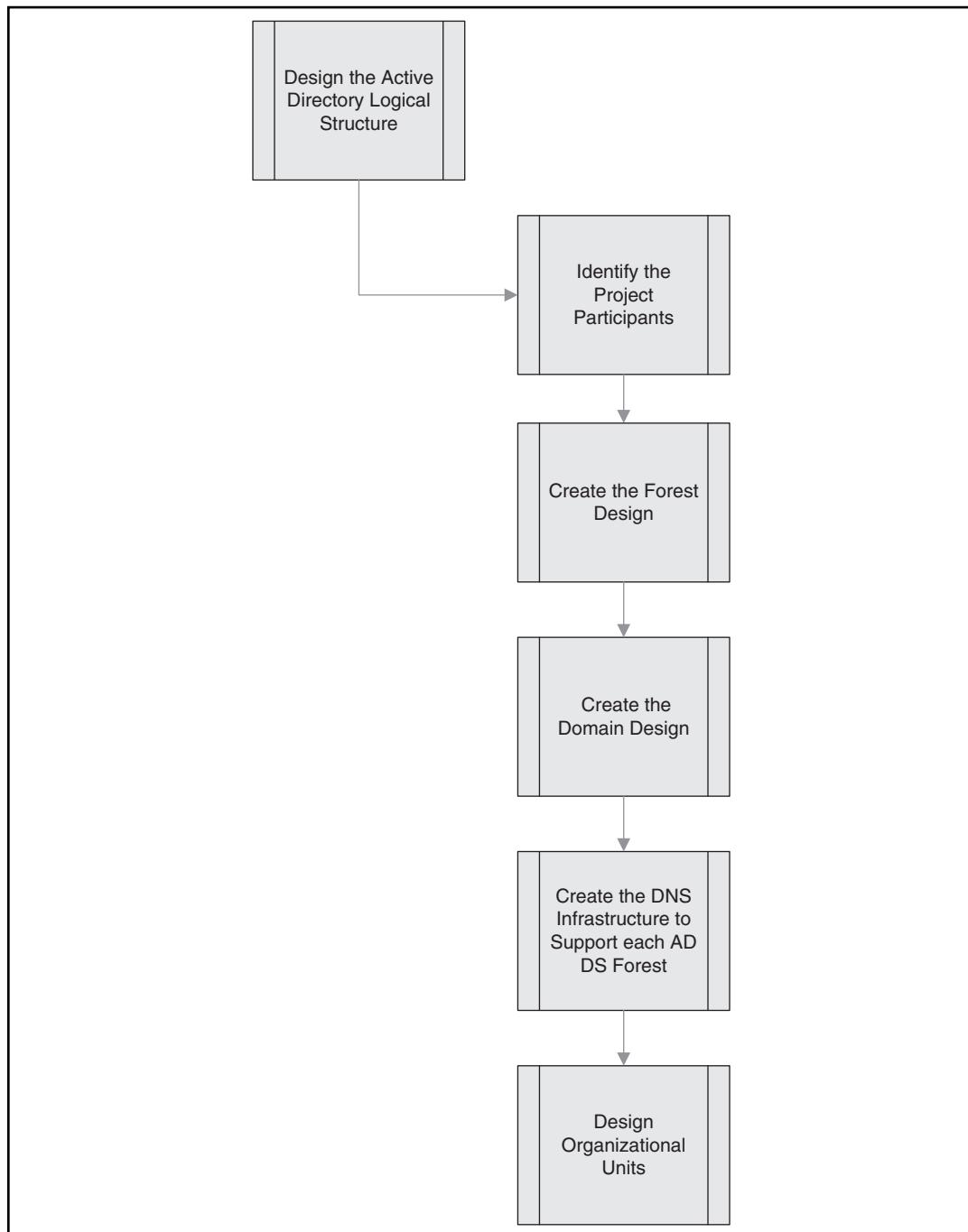
the directory database, or the Active Directory forest. Partitioning data enables organizations to replicate data only to where it is needed. That is, replicating objects, like schema objects, to other domain controllers in the forest, or objects, such as account password changes, to just those in the AD domain. In this way, the directory can scale globally over a network that has limited available bandwidth. In addition, the domain supports a number of other core functions related to administration, including:

- **Network-wide user identity** As we have already discussed, users can log onto their workstation in any domain and gain access to resources on any server in any domain, assuming they have the appropriate permissions.
- **Authentication** Domain controllers provide authentication services for user accounts and supply additional authorization data such as group membership, which can be used to track access to resources across the network.
- **Trust relationships** Allow users outside the domain to authenticate and gain access to resources securely.
- **Replication** The domain partition of the directory database replicates domain objects, such as new users, or changes to existing accounts, to other domain controllers in the domain; each domain controller holds a write-able copy of this partition (except the read-only domain controller or RODC) and therefore are all able to initiate this replication.

Organizational Units (OU)

OUs are used to group objects for administrative purposes, such as assigning group policies or delegating administrative control. Think of the OU like a folder in Windows Explorer. You could save each and every file to the root of your C:\ partition if you chose; but managing the files, and those who access the files, would be a nightmare. The same goes for Active Directory. Organizing security objects into OUs makes administration more efficient; you can create a group policy object (GPO) that applies to a group of users by placing all of the users into a certain OU, and then link the GPO to the OU. Control of the OU (and all of the objects within the OU) is determined by access control lists (ACLs). Managing control by using ACLs is efficient because it allows an administrator to delegate full or even limited control of an OU to a user or group of users trusted to perform administrative tasks. Figure 3.5 shows the steps used in creating the Active Directory logical structure.

Figure 3.5 The High-Level Steps in Creating the Active Directory Logical Structure



The Active Directory Domain Services (AD DS) Physical Design Structure

The Active Directory physical design involves knowing what hardware you have available to create AD DS servers, and knowing how your network subnets are mapped. Active Directory uses sites, site links, and subnet objects to determine when replication should happen, if it should be compressed, which global catalog server will respond to a client's query, which Domain Controller will authenticate a user's logon request, and so on. The proper planning of these sites will make more efficient use of available network bandwidth, and make queries and logons much quicker. The following elements make up the physical design: domain controllers, sites and site links, and subnets.

Domain Controllers

The Active Directory partitions that make up the DS database are stored on domain controllers. Windows Server 2008 has a new type of domain controller, which holds a read-only copy of the directory database. This domain controller, the RODC, is primarily used in branch offices, but can be used throughout your organization.

NOTE

For more information on the RODC, please read Chapter 6.

TEST DAY TIP

If you will be deploying a domain controller in a branch office where physical security is at a minimum, consider using the RODC.

Sites and Site Links

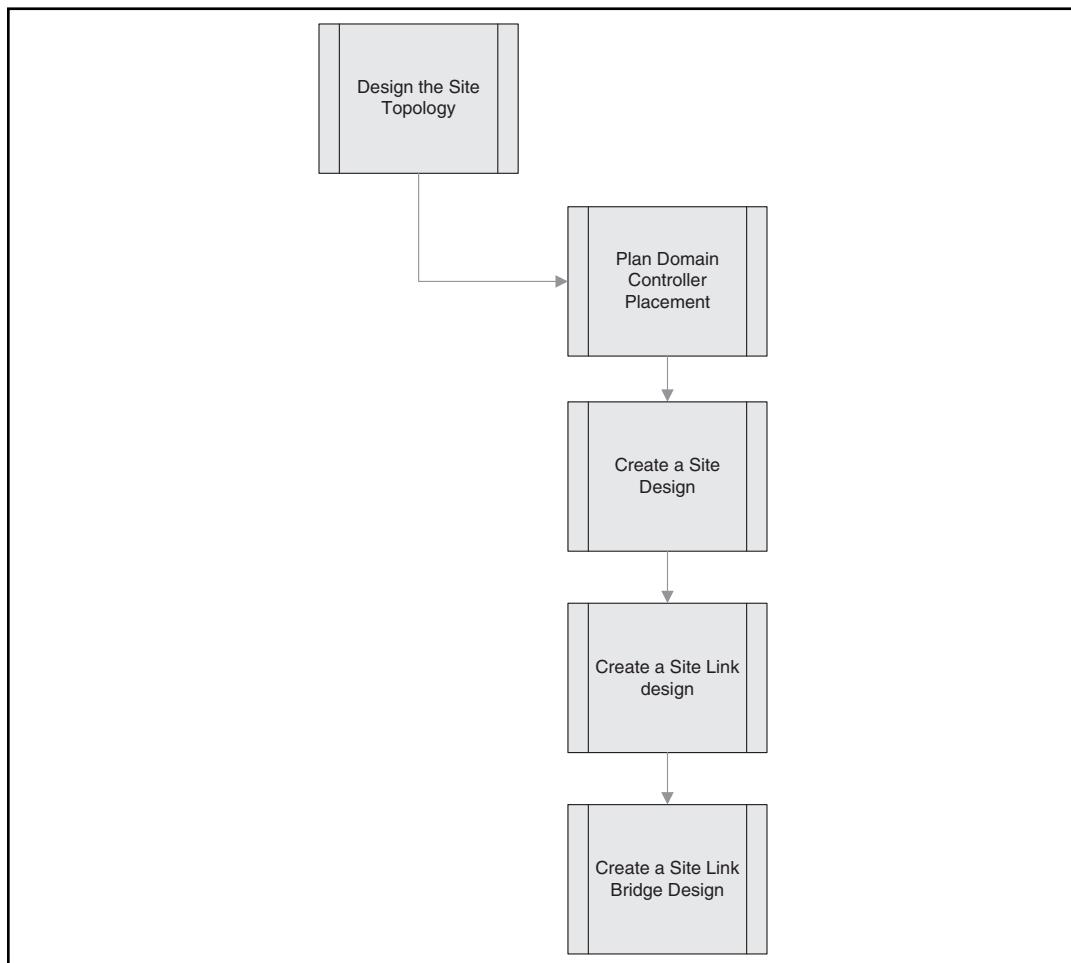
Active Directory domain controllers do not know what city or state they are in, or even what country. They rely on the Active Directory Sites to let them know where they are located in relation to other domain controllers. The site is the logical map of the physical network. The site is defined by subnet objects and site links, which

are logical links that use your normal routing table to route queries and replication traffic to other parts of your physical network. Sites are made up of subnet objects, and let services like DNS “know” where you are in relation to domain controllers. This “knowledge” allows DNS to find global catalog servers close to you to make querying Active Directory more efficient.

Subnets

Subnets tell Active Directory where on the physical network a domain controller, workstation, printer or other device is located. The subnet is defined by the actual IP subnet, and a Location attribute. Windows Server 2008 Sites support both IPv4 and IPv6 subnets. Figure 3.6 shows the steps for creating the site topology.

Figure 3.6 High-Level Steps in Creating the Site Topology



Creating the Forest Root Domain

Deploying your forest root domain is the first step in deploying Active Directory Domain Services (AD DS) in your organization. The forest root domain is the first domain created in your forest. This provides the foundation for your AD DS forest infrastructure. During the forest root domain deployment, you begin to implement the Active Directory design that your design team has provided, including the domain name system (DNS) infrastructure that AD DS requires. In addition, services that run on forest root domain controllers, such as the Kerberos authentication protocol, must be highly available to ensure that users maintain access to resources throughout the forest.

If your AD DS forest design requires only one domain, then the forest root domain will also contain all of your users, groups, device and other resources. During deployment, you can create an organizational unit (OU) structure to make group policy and delegation of control more efficient, after the forest root domain deployment is complete.

In a multiple AD DS domain design, the forest root domain can be a dedicated root used only for administration of the forest and for pass-through authentication, or it can contain users, groups, and resources in addition to the forest administration accounts, the schema administrator and the enterprise administrator. After you deploy the forest root domain, the enterprise administrator will create one or more child domains to complete the AD DS forest.

Windows Server 2008 comes with three different ways to install AD DS: The Windows Interface, which itself has two different wizards to assist with this, the command prompt, and finally, by using an answer file.

EXERCISE 3.2

INSTALLING THE AD DS USING THE WINDOWS INTERFACE

The Windows Interface comes with two different wizards to assist with the deployment of AD DS. They are Server Manager's Add Roles Wizard and DCPROMO.exe. To use either of these, you must be logged on as an administrator, and you should have a password set. Depending on which version of Server 2008 you installed, you may not have a password set. To set the password from the command prompt, type net user Administrator P@ssw0rd /passwordreq:yes (where P@ssw0rd is a strong password). Once the password has been set, log on as the administrator, and then follow these steps:

1. Click **Start**, and then click **Server Manager**.
2. In **Roles Summary**, click **Add Roles**.
3. Review the information on the **Before You Begin** page and then click **Next**.
4. On the **Select Server Roles** page, click the **Active Directory Domain Services** check box, and then click **Next**.
5. Review the information on the **Active Directory Domain Services** page, and then click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**.
7. On the **Installation Results** page, click **Close** to close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).
8. On the **Welcome to the Active Directory Domain Services Installation Wizard** page, click **Next**. *NOTE:* You can select the **Use advanced mode installation** check box to get additional installation options.
9. On the **Operating System Compatibility** page, review the warning about the default security settings for Windows Server 2008 domain controllers, and then click **Next**.
10. On the **Choose a Deployment Configuration** page, click **Create a new domain in a new forest**, and then click **Next**.
11. On the **Name the Forest Root Domain** page, type the full Domain Name System (DNS) name for the forest root domain, and then click **Next**.
12. If you selected **Use advanced mode installation** on the **Welcome** page, the **Domain NetBIOS Name** page appears. On this page, type the NetBIOS name of the domain, if necessary, or accept the default name and then click **Next**.
13. On the **Set Forest Functional Level** page, select the forest functional level that accommodates the domain controllers that you plan to install anywhere in the forest, and then click **Next**. *NOTE:* If you select any forest functional level other than Windows Server 2008, the **Set Domain Functional Level** page appears next.
14. On the **Set Domain Functional Level** page, select the domain functional level that accommodates the domain controllers that you plan to install anywhere in the domain, and then click **Next**.

15. On the **Additional Domain Controller Options** page, DNS server is selected by default so that your forest DNS infrastructure can be created during AD DS installation. If you plan to use Active Directory–integrated DNS, click **Next**. If you have an existing DNS infrastructure and you do not want this domain controller to be a DNS server, clear the **DNS Server** check box, and then click **Next**. *NOTE:* If the wizard cannot create a delegation for the DNS server, it displays a message to indicate that you can create the delegation manually. To continue, click **Yes**.
16. On the **Location for Database, Log Files, and SYSVOL** page, type or browse to the volume and folder locations for the database file, the directory service log files, and the SYSVOL files, and then click **Next**. *NOTE:* Windows Server Backup backs up the directory service by volume. For backup and recovery efficiency, store these files on separate volumes that do not contain applications or other non-directory files.



TEST DAY TIP

Even though Step 18 mentions DSRM, AD DS is now a service in the Services.msc. Most offline tasks can be completed by stopping this service and going to a command prompt without having to reboot into Directory Services Restore Mode.

17. On the **Directory Services Restore Mode Administrator Password** page, type and confirm the restore mode password, and then click **Next**. This password must be used to start AD DS in Directory Service Restore Mode (DSRM) for tasks that must be performed offline.
18. On the **Summary** page, review your selections. Click **Back** to change any selections, if necessary, or click **Next**. *NOTE:* To save the selected settings to an answer file that you can use to automate subsequent AD DS operations, click **Export** settings. Type the name for your answer file and then click **Save**.
19. You can either select the **Reboot on completion** check box to have the server restart automatically or you can restart the server to complete the AD DS installation when you are prompted to do so.



TEST DAY TIP

To create an Answer File that will automatically install AD DS without any prompts, follow the aforementioned detailed steps, and then on Step 20 select **Export Settings** and **Save the Answer File**. An Answer File would be required to install AD DS on a server core installation or by using a command prompt.

Forest and Domain Function Levels

In Windows Server 2008, AD DS makes it possible for you to introduce advanced features into your environment by raising the domain or forest functional levels. To use advanced AD DS features, you must identify the operating systems that are running on the domain controllers in your environment. You must also determine the best functional level for your organization based on your existing infrastructure and then raise the domain or forest functional level as appropriate. You can raise the functional level when all domain controllers in the domain or forest are running an appropriate version of Windows. Although raising the functional level makes it possible for you to enable new features, it also limits the versions of Windows operating systems that you can run on domain controllers in your environment. Remember, these requirements are domain controller specific; so if you are running Windows Server 2003 on your file servers, and Windows Server 2008 on all of your domain controllers, then you should raise the domain and forest function levels to Server 2008. Table 3.1 will help you understand the operating system requirements of each function level.

Table 3.1 Features Available at Each Forest Function Level

| Forest Function Level | Operating Systems Supported | Features Available |
|-----------------------|---|--|
| Windows 2000 Native | Windows 2000 Server Windows Server 2003 Windows Server 2008 | All default AD DS features supported |
| Windows Server 2003 | Windows Server 2003 Windows Server 2008 | All default AD DS features Forest trust |

Continued

Table 3.1 Continued. Features Available at Each Forest Function Level

| Forest Function Level | Operating Systems Supported | Features Available |
|-----------------------|-----------------------------|---|
| Windows Server 2008 | Windows Server 2008 | Domain rename Linked-value replication RODC deployment Convert inetOrgPerson object into User object Create LDAP query groups Deactivation and redefinition of schema attributes and classes All of the above features, plus each domain will function in Server 2008 domain function level |

When you deploy AD DS, set the domain and forest functional levels to the highest value that your environment can support (see Table 3.1). This way, you can use as many AD DS features as possible. For example, if you are sure that you will never add domain controllers that run Windows Server 2003 to the domain or forest, select the Windows Server 2008 functional level during the deployment process. However, if you might retain or add domain controllers that still run Windows Server 2003, select the Windows Server 2003 functional level.

When you deploy a new forest, you are prompted to set the forest functional level, and then set the domain functional level (see Step 13 in the section Creating the Forest Root Domain earlier in this chapter). You cannot set the domain functional level to a value that is lower than the forest functional level. For example, if you set the forest functional level to Windows Server 2008, you can set the domain functional level only to Windows Server 2008. The Windows 2000 native and Windows Server 2003 domain functional level values are not available on the **Set domain functional level** page of the Active Directory Domain Services Installation Wizard. In addition, all domains that you subsequently add to that forest have the Windows Server 2008 domain functional level by default (see Table 3.2 for features available at the domain function levels).

Table 3.2 Features Available at Each Domain Function Level

| Domain Function Level | Operating Systems Supported | Available Features |
|-----------------------|---|--|
| Windows 2000 Native | Windows 2000 Server Windows Server 2003 Windows Server 2008 | All default AD DS features Universal groups group nesting group conversion (converting between security and distribution group) SID history |
| Windows Server 2003 | Windows Server 2003 Windows Server 2008 | All default AD DS features Domain rename using netdom.exe Logon time stamp updates Redirect default Users and Computers containers in AD Ability for Authorization Manager to store authorization policies in AD DS Constrained delegation (applications can take advantage of secure delegation of user credentials using Kerberos) Selective Authentication; specify which users and groups from trusted forests can authenticate) |
| Windows Server 2008 | Windows Server 2008 | All of the above DFS replication for Windows Server 2003 SYSVOL Advanced Encryption Standard for Kerberos Last interactive logon information Fine-grained password policies |



TEST DAY TIP

Remember, you specify the forest function level while installing the forest root domain. Once set, you cannot set it to a lower value; so if you will have Windows Server 2003 domain controllers do not set this at Windows Server 2008 forest function level.

Follow these guidelines for raising your forest function levels:

- You must be a member of the Enterprise Admins group to raise the forest function level.
- You can use Active Directory Domains and Trusts to raise the forest function level.
- You can raise the forest function level on the schema operations master only. If you attempt to raise it on a different DC, Active Directory Domains and Trusts will automatically target the schema master with the change.
- You can raise the forest function level only if all DCs in the forest run the version of the operating system supported by that level.
- You cannot lower the forest function level after you have raised it.
- You cannot reverse the operation of raising the forest function level. If you need to revert back down to a lower function level, you must rebuild the forest or restore it from a backup copy.

Follow these guidelines for raising the domain function levels:

- You must be a member of the Domain Admins group to raise the domain function level.
- You can use either Active Directory Domains and Trusts or Active Directory Users and Computers to raise the domain function level.
- You can raise the domain function level on the primary domain controller (PDC) emulator operations master only. If you attempt to raise it on a different DC, the AD DS tool you use will automatically target the PDC emulator.
- You can raise the domain function level only if all DCs in the domain run the version of the operating system supported by that level.

- You cannot set a domain function level value that is lower than the forest function level.
- You cannot lower the domain function level once you have raised it.
- You cannot reverse the raising of the domain function level. If you must revert back to a lower function level, you must rebuild the domain or restore from a backup copy.

Upgrading Your Forest

Before you can raise domain and forest functional levels, you have to evaluate your current environment and identify the functional level requirement that best meets the needs of your organization. Assess your current environment by identifying the domains in your forest, the domain controllers that are located in each domain, the operating system that each domain controller is running, and the date that you plan to upgrade the domain controllers. Certain situations may prevent you from upgrading from an earlier version of Windows to Windows Server 2008 function levels:

- Insufficient hardware
- A DC running an anti-virus program which is incompatible with Windows Server 2008
- Use of an application or other program on your DC that is incompatible with Windows Server 2008

After assessing your environment, you have to identify the function level upgrade that best applies to your situation. Your options are:

- Windows 2000 native mode Active Directory to Windows Server 2008 AD DS
- Windows Server 2003 forest to Windows Server 2008
- New forest

Windows 2000 Native Mode Active Directory to Windows Server 2008 AD DS

If your Windows 2000 AD environment contains all Windows 2000 DCs, and was already set to Windows 2000 native mode, then the domain and forest function levels are automatically set to Windows 2000 native mode domain and forest function levels. To take advantage of the advanced features available in Windows Server 2008 AD DS, you will need to upgrade your domains and then your forest. You can do this one of two ways:

- Install Windows Server 2008 on new servers, install AD DS, and join them to the Windows 2000 Active Directory environment. Then retire all Windows 2000 DCs (or upgrade them). Manually raise the domain and forest function levels to Windows Server 2008.
- Upgrade all Windows 2000 domain services to Windows Server 2003. Then do an in-place upgrade of these servers to Windows Server 2008. Manually raise the domain and forest function levels to Windows Server 2008.



NOTE

If you want to get the added benefits of Windows Server 2008 domain function level, but will still have Windows Server 2000 domains in the forest, do not raise the forest function level. Instead, raise the domain function levels for those domains that have only Windows Server 2008 Domain Controllers, and leave the forest function level at Windows 2000.

Windows Server 2003 Forest to Windows Server 2008

If your Windows Server 2003 AD environment contains all Windows Server 2003 DCs, then the function levels are automatically set to Windows 2000 native domain function level and Windows 2000 forest function level. To take advantage of the advanced features available in Windows Server 2008 AD DS, you will need to upgrade your domains and then your forest. You can do this in one of two ways:

- Install Windows Server 2008 on new servers, install AD DS, and join them to the Windows 2000 Active Directory environment. Then retire all Windows 2000 DCs (or upgrade them). Manually raise the domain and forest function levels to Windows Server 2008.
- Perform an in-place upgrade of these servers to Windows Server 2008. Manually raise the domain and forest function levels to Windows Server 2008.

New Forest

When you create a new forest using the Windows Server 2008 operating system on the server, the function levels are automatically set to Windows 2000 native mode domain function level and Windows 2000 forest function level. This allows you to retain your Windows Server 2000 and Windows Server 2003 DCs during the transition. Once all DCs have been upgraded to Windows Server 2008, and you are certain there will be no more servers introduced as DCs running an earlier version of Windows, then you may raise the forest function level. Doing so will automatically raise the domain function level.

Intra-Organizational Authorization and Authentication

First, there is a difference between authorization and authentication. This section will separate these two terms and describe each. Then we will go into the way Windows Server 2008 deals with intra-organizational authorization and Authentication.

Authorization is the process of determining which activities are permitted. In Windows Server 2008, that typically comes in the form of NTFS permissions on a folder, or access control lists (ACLs) in AD DS. In other words, authorization is the act of being allowed to do something. Authentication, on the other hand, is a security measure which proves you are who you say you are, when attempting to do something, such as log on to a network, access a shared folder or change a user's password. Typically, we think of these terms as one in the same. When we think of authentication, we automatically think authorization.

In a Windows Server 2008 forest, all domains in all trees are automatically trusted through a two-way transitive trust relationship. That means that every user in the domain can get authenticated against their DC, and be authorized to access any folder in the forest, regardless of which server it resides on. This authentication happens through a security protocol known as Kerberos. Kerberos was developed by MIT and has been around for a long time, even before Active Directory in Windows 2000.

All Kerberos connections include three different parties: the client requesting the connection, the server that holds the requested data, and the Kerberos Key Distribution Center (KDC) which holds the keys that will secure the data transmissions. In Windows

Server 2008 and Windows Vista, significant security enhancements were added to Kerberos. These include:

- Advanced Encryption Standard (AES) Support
- Improved security for KDCs located on branch office domain controllers. In Windows Vista and Windows Server 2008, this security enhancement enables the use of AES with the Kerberos authentication protocol. This is an improvement over Windows XP and includes the following changes:
 - **AES support for the base Kerberos authentication protocol** The base Kerberos protocol now includes support for AES for encryption of ticket-granting tickets (TGTs), service tickets, and session keys.
 - **AES support for the generic security services (GSS) Kerberos mechanism** Not only is there AES support for the base Kerberos protocol, but GSS messages are protected with AES as well (GSS message conduct the client/server communications in Windows Vista and Server 2008).

Typically speaking, if all of your clients are using Windows Vista, and all of your servers are running Windows Server 2008, all communication will take place using AES. However, if your clients and servers are running operating systems earlier than Windows Vista and Server 2008, the exchange will not use AES, and the following exchange will take place:

- **TGT** A ticket granting ticket is created by the KDC and sent to the client, if authentication to the KDC succeeds.
- **Service ticket** A service ticket is created by the KDC and sent to the client. The client then sends it to the server to establish authentication of the client.
- **AS-REQ/REP (Authentication Service Request/Response)** This is the Kerberos TGT request and reply message sent to the KDC from the client. If successful, the KDC will grant a TGT to the client.
- **TGS-REQ/REP (Ticket-Granting Service Request/Response)** This is the Kerberos service ticket request and reply messages sent from the client to the KDC when it is instructed to obtain a service ticket for the server.
- **GSSAPI (Generic Security Service API) and GSS-SPNEGO (GSS Negotiate Support Provider)** The GSSAPI and GSS-SPNEGO mechanisms negotiate a secure context for sending and receiving messages during these key exchanges.

Use Table 3.3 to determine if AES will be used in the exchange between the different Windows operating systems:

Table 3.3 AES and the Different Windows Operating Systems

| Client | Server | KDC | Ticket/Message encryption |
|----------------------------|----------------------------------|----------------------------------|---|
| Earlier than Windows Vista | Earlier than Windows Server 2008 | Windows Server 2008 | TGT may be encrypted with AES based on policy |
| Earlier than Windows Vista | Windows Server 2008 | Windows Server 2008 | Service ticket encrypted with AES |
| Windows Vista | Windows Server 2008 | Windows Server 2008 | All tickets and GSS encrypted with AES |
| Windows Vista | Windows Server 2008 | Earlier than Windows Server 2008 | GSS encrypted with AES |
| Windows Vista | Earlier than Windows Server 2008 | Windows Server 2008 | AS-REQ/REP and TGS-REQ/REP encrypted with AES |
| Earlier than Windows Vista | Windows Server 2008 | Earlier than Windows Server 2008 | No AES |
| Windows Vista | Earlier than Windows Server 2008 | Earlier than Windows Server 2008 | No AES |
| Earlier than Windows Vista | Earlier than Windows Server 2008 | Earlier than Windows Server 2008 | No AES |

TEST DAY TIP

Because of the two-way transitive trust relationship between all domains in a forest, if all of your clients are running Windows Vista and all of the servers are running Windows Server 2008, it makes no difference which domain they are in. This process will be secure. Also, if your forest is at Windows Server 2003 or later, you can take advantage of cross-forest trusts to get this added security for external users.

Schema Modifications

The Active Directory schema contains the definitions of every object class and attribute that can be created in AD DS. The following make up the Active Directory schema elements:

- **Class** A formal description of an identifiable type of object stored in the directory service, such as User or Group.
- **Attributes** Describe the objects that are represented by the classes defined in the schema. These are listed separately than classes which allows a single attribute to be applied to many objects, such as Description field in a group or printer object.
- **Object** A unit of data storage in the directory service. For example, a user is an object that belongs to the class users.

There are many reasons to make modifications to the Active Directory schema. Some of these reasons include installing a directory enabled application, such as Microsoft Exchange Server or System Center Configuration Manager (SCCM) 2007, or to prepare your forest for an upgrade. If you are installing Windows Server 2008 on a fresh computer, and then installing AD DS, no schema modifications will be necessary. However, before you can add a domain controller that is running Windows Server 2008 to an Active Directory environment running an earlier version of Windows, you must update the Active Directory schema first, on the DC that runs the schema master operations master role. Use the following points when updating the Windows 2000 or Server 2003 schema for Windows Server 2008:

- **Administrative Credentials** You must be a member of all the following groups to modify the schema: Enterprise Admins, Schema Admins, and Domain Admins for the domain that contains the schema master (typically the forest root domain).
- **Schema Master** You must modify the schema while bound to the DC holding the schema master operations master role token.

EXERCISE 3.3

MODIFYING THE ACTIVE DIRECTORY SCHEMA

To modify the schema to prepare for the addition of Windows Server 2008 Domain controllers, follow these steps:

1. Log on to the schema master as a member of the groups listed in the administrative credentials section above (or use the Runas command when launching the command prompt).
2. Insert the Windows Server 2008 DVD into the CD or DVD drive. Copy the contents of the `\sources\adprep` folder to an **Adprep** folder on the schema master, for example to the C:\ drive so that the path to the files inside the folder is C:\Adprep.
3. Open a command prompt and change directory to the C:\Adprep directory.
4. At the command prompt, type `adprep /forestprep` and then press **Enter**.
5. If you plan to install an RODC into any domain on the forest, type `adprep /rodcprep` and then press **Enter**.

Allow the operations to complete and replicate to all DCs in the forest prior to installing AD DS on Windows Server 2008. Sometimes it might be necessary not only to modify the schema but also to just view the schema. To view the schema we can use an MMC snap-in called Active Directory Schema. This snap-in is “hidden” by default and is not accessible. Follow these steps to register and load the snap-in into your MMC console:

1. From a command prompt opened with elevated privileges, type `c:\windows\system32\regsvr32 schmmgmt.dll` and then press **Enter**.
2. In the **regsvr32** dialog box click **OK**.
3. At the command prompt, type `MMC` and then press **Enter**.
4. From the **File** menu, click **Add/Remove Snap-in**.
5. From the list of available snap-in, click **Active Directory Schema**, and then click **Add** and **OK**.
6. Save the MMC console.



TEST DAY TIP

Even though it is not possible to delete a schema object, as long as the Forest is set to Windows Server 2003 or above function level, you can deactivate or even redefine a schema object. Lower forest function levels can disable a schema object, but cannot delete, deactivate or redefine one.



NOTE

It is a good practice to unregister the schmmgmt.dll DLL file once you are done viewing the Active Directory Schema snap-in. You can unregister it by typing **regsvr32 schmmgmt.dll /u** at the command prompt. Unregistering it ensures that no other administrators may launch Active Directory Schema and make modifications.

Designing an Active Directory Topology

In the last section, we concentrated on the Active Directory terminology, function levels, getting ready to deploy Windows Server 2008 Active Directory Domain Services in your enterprise, and modifying your AD schema. In this section we will take a look at server placement, your Active Directory site and replication topology, and your printer location policies.

Before we start on server placement, however, we first need to discuss the roles of the servers that you can deploy with Windows Server 2008, such as the different operations master token holders, and discuss the Active Directory physical topology.

Active Directory Domain Services (AD DS) supports multi-master replication of directory data, which means any domain controller can accept directory changes from any domain controller and replicate the changes to all other domain controllers. However, certain changes, such as schema modifications, are impractical to perform in a multi-master fashion. For this reason certain domain controllers, known as operations masters, hold roles responsible for accepting requests for certain specific changes.



TEST DAY TIP

Operations master role holders must be able to write some information to the Active Directory database. Because of the read-only nature of the Active Directory database on a read-only domain controller (RODC), RODCs cannot act as operations master role holders.

Operations masters are also known as flexible single master operations, or FSMO token holders.

There are a total of five operations master role tokens available in AD DS: two of these forest-wide, that is regardless of how many domains are deployed in your forest, there will be only one domain controller holding this token, and three of these are domain-wide, that is regardless of how many domain controllers are deployed in your domain, there will be only one holding this token. The operations master roles include forest-wide (one per forest) and domain-wide (one per domain).

Forest-wide roles include these two DCs:

- **Schema Master** This DC governs all changes made to the AD schema, and replicates these changes to its replication partners, who further replicate the change to all DCs in the forest.
- **Domain-Naming Master** This DC governs the addition and removal of domains from the forest, as well as other directory partitions (DNS application partition, for example).

Domain-wide roles include these features:

- **PDC Emulator** The primary domain controller (PDC) emulator is responsible for the following functions in the domain: master browser, time-sync for all domain members, and password changes
- **Infrastructure Master** Maintains a list of users from other domains that are members of groups in its domain.
- **RID Master** The relative identifier (RID) master is responsible for maintaining a global (domain-wide) pool of RIDs for all of the DCs in the domain. When a new security principal such as a user or group is created in the domain, it gets a security identifier (SID) from a DC. This SID is made up of a RID plus a domain's SID. To ensure that no two multi-master DCs assign the same SID to two different security principals, the RID master assigns the available RIDs to each DC.

Server Placement

Once you have documented all the network information that will be used to create your site topology, such as all of your IP subnets, physical locations and physical links between your locations, you need to decide where to place all of your domain controllers, including your forest root domain controllers, your regional domain controllers, your operations master role holders, and your global catalog servers.

Determining the Placement of the Forest Root Domain Controllers

As we have learned earlier in the chapter, forest root domain controllers run key services, such as the Kerberos authentication protocol, and are used to create transitive trusts between the domains in your forest. These are necessary for the users that will need to access resources in other domains. Therefore, place forest root domain controllers in central locations and at locations that host datacenters. If users in one location need to access resources from another domain that is in the same physical location, and the network availability between the data center and the user location is unreliable, you can either add a forest root domain controller in the user's location or create a shortcut trust between the two domains.



TEST DAY TIP

Shortcut trusts offer a way to optimize authentication requests made by users in either domain.

Determining the Placement of the Regional Domain Controllers

Place regional domain controllers for each domain in each central location. After placing regional domain controllers in all central locations, evaluate the need for placing regional domain controllers at branch locations. Removing the need for branch office domain controllers from remote locations reduces the support and hardware costs required to maintain a remote server infrastructure. Also, ensure the physical security of domain controllers in hub and satellite locations so that unauthorized personnel cannot access them. Do not place writable domain controllers in any locations in which you

cannot guarantee the physical security of the server. A person who has physical access to a writable domain controller can compromise the system by:

- Removing or replacing the physical disk on the DC
- Installing a second operating system (OS) on the domain controller, booting to that other OS, and accessing the SYSVOL on the DC
- Gaining access to, and possibly manipulating, the system state backup.

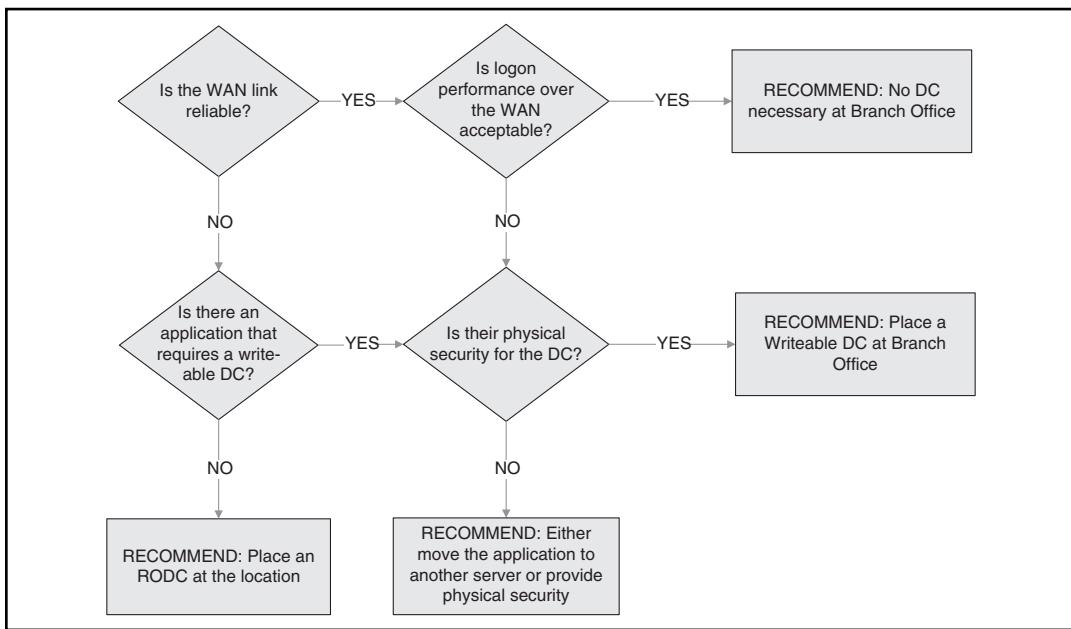


TEST DAY TIP

Consider using an RODC at your branch locations, or at locations in which physical security is at a minimum.

See Figure 3.7 for an idea of where to place a DC, or what kind of DC to place, at remote locations. Some other issues to consider with regard to placing your Regional Domain Controllers include:

- **Onsite IT Staff** If you do not have onsite IT staff, but require a regional domain controller, consider using RODC and administrator-role separation.
- **WAN Link Availability** If you have a Wide-Area Network (WAN) link that is unreliable, consider using a regional domain controller in each location where users frequently log on.
- **Authentication Availability** Certain applications may require users be authenticated at all times.
- **Logon Performance over WAN Links** If the logon performance is unacceptable at times over the WAN links, such as early in the morning when everyone is logging on over the WAN link.
- **Number of Users in Each Location** Typically speaking, an office with more than 100 users should have a domain controller. Of course that number will vary depending on many factors, such as WAN link speed, user profiles, how many network resources are accessed by the users, and so on.
- **Logon Traffic vs. Replication Traffic** Once you have determined that the logon or authentication performance is unacceptable, and you have decided to place a domain controller in that location, consider the added replication traffic that has just been introduced over the WAN.

Figure 3.7 What Kind of DC to Place in Regional Locations

Determining the Placement of the Operations Masters

Carefully plan which piece of hardware, that is which server, will become the first domain controller in your domain or forest. When AD DS is installed in a new domain, that domain controller will hold all of the domain-wide operations master tokens. When that domain is the first domain in a new forest, then it also holds the forest-wide roles, plus the global catalog. These automatic operations master role assignments can cause very high CPU usage on the first domain controller created in the forest or the domain. To avoid this, assign (transfer) operations master roles to various domain controllers in your forest or domain. Place the domain controllers that host operations master roles in areas where the network is reliable and where the operations masters can be accessed by all other domain controllers in the forest. See Figure 3.8 for an example of when the operations masters may be inaccessible to some of your domain controllers.

Out of all of the operations masters, certain DCs will see more action than other DCs. For example, once your forest is created, and all of the domains have been created, and all of the sites, site links and subnet objects have been created, the domain naming

master will have little to do by itself. Likewise, the schema master will have little to do, unless you plan to make schema modifications. But other operations masters are busy all the time. And the placement of these operations master is important. Planning the placement can mean a reliable infrastructure, or an unreliable infrastructure. The points are important in your design decisions:

- Placement of the PDC emulator
- Placement of the infrastructure master
- Planning for networks with limited connectivity

Placement of the PDC Emulator

As we have discussed, the PDC emulator processes client password changes. There can only be one PDC emulator in each domain. Even if all the domain controllers are upgraded to Windows 2000, Windows Server 2003, and Windows Server 2008, and the domain is operating at the Windows 2000 native functional level, the PDC emulator receives preferential replication of password changes performed by other domain controllers in the domain. If a password was recently changed, that change takes time to replicate to every domain controller in the domain. If logon authentication fails at another domain controller due to a bad password, that domain controller forwards the authentication request to the PDC emulator before deciding whether to accept or reject the logon attempt.

Therefore, you should place the PDC emulator in a location that contains a large number of users from that domain for password forwarding operations if needed. In addition, ensure that the location is well connected to other locations to minimize replication latency.

Placement of the Infrastructure Master

This is a great definition of what the infrastructure master does: It resolves inconsistencies for cross-domain referenced objects. Let's that break down. Cross-domain referenced objects are security principals in one domain that belong to a group in another domain. For example, DomainA\JaneDoe belongs to DomainB\ResourceAccess-DL. JaneDoe is a cross-domain referenced object. As far as DomainB is concerned she has a SID that maps to DomainA\JaneDoe. Let's go to the next step and say that Jane gets married, and so her Domain Administrator goes through the proper steps of changing her name in AD DS. She is now DomainA\JaneSmith. Because this change is in the Domain partition in AD DS, that change replicates to all DCs in DomainA, but not

to the DCs in other domains. Next time she tries to access a file in DomainB that she has access to, the DC will see that the SID does not match the name anymore. This is an inconsistency. So now we have an inconsistency with a cross-domain referenced object. This is where the infrastructure master comes in.

To resolve this inconsistency, the infrastructure master constantly monitors group memberships, looking for users and other security principals from other domains. If it finds one, it checks with the user's domain to verify that the information is up to date. If the information is out of date, the infrastructure master updates the information and then replicates the change to its replication partner, and eventually to all of the other domain controllers in its domain. This is true except in the following situations:

- **If all domain controllers are global catalog servers** If all DCs are also global catalogs servers, then the infrastructure master token doesn't function at all, since all global catalogs hold domain partitions of all domains, and therefore there are no inconsistencies.
- **If the forest has only one domain** In a single-domain forest, cross-domain referenced objects.

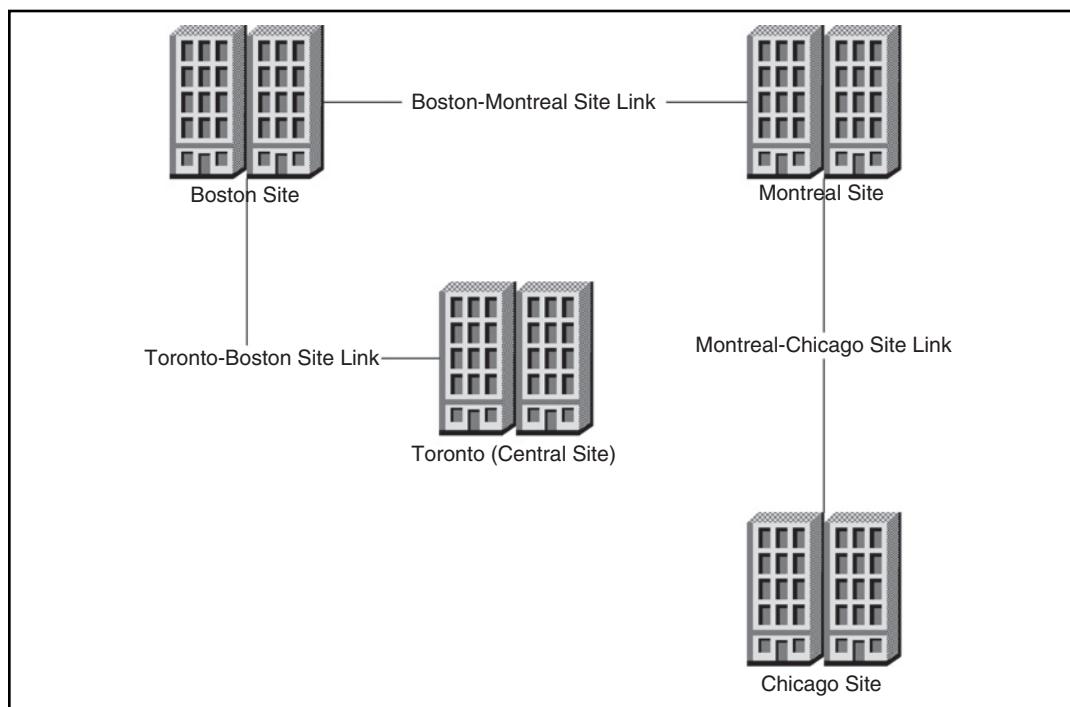


TEST DAY TIP

Do not place the infrastructure master token on a global catalog. If you do then the infrastructure master will not function. Therefore, if you create a new domain in a new forest and need to make sure that all operations masters are functioning, transfer the infrastructure master to another DC.

Planning for Networks with Limited Connectivity

If your environment has a central location in which you can place all of the operations masters, certain domain controller functions that depend on the availability of those operations master role holders might be affected. For example, if an organization creates sites Toronto, Boston, Montreal, and Chicago, then site links exist between Toronto and Boston, between Boston and Montreal, and between Montreal and Chicago. See Figure 3.8.

Figure 3.8 Sites and Operations Master Limitations

Routing tables mirror the connectivity of the sites links. In this example, all operations master roles are placed in Toronto and the option to **Bridge all site links** is not selected. Replication monitoring will result in successful replication between all of the sites. However, the operations master role functions will have the following limitations:

- Domain controllers in Chicago can only access their replication partners in Montreal, so they cannot reach the operations master DCs that have all been placed in Toronto. This could result in a user being denied logon due to a recent password change, or a domain controller running out of its RID pool.
- Domain controllers in Montreal can only reach their replication partners in Boston and Chicago, and therefore cannot reach the operations master DCs in Toronto. This could result in an application not getting installed properly because it could not find the schema operations master or having the ability to install a custom application partition.



TEST DAY TIP

In Active Directory Sites and Services, **Bridge all Site Links** is selected by default. If you keep this option selected, all sites will be virtually linked to all other sites, and these issues would not occur.

Determining the Placement of Global Catalog Servers

In a single domain forest, this is simple. Each DC should be a global catalog (GC) server. This is because in a single domain each DC already holds the domain partition; so configuring all DCs as GCs would result in no extra disk space, no extra replication traffic and no extra CPU utilization on the DC. However, in this scenario, only the first DC created in the forest will hold the GC role, so you would need to manually add that role to the other DCs upon installation of AD DS. So even though any DC can answer authentication requests, only the DC designated as a GC can answer a global catalog query, such as Find Printers. You can add the global catalog role by using Active Directory Sites and Services.



TEST DAY TIP

Global catalog servers answer requests on TCP Port 3268.

To determine what information gets stored and replicated on global catalog servers, or to change what data is being stored and replicated, open **Active Directory Schema**, expand **Attributes**, and then right-click the attribute you would like to modify and click **Properties**. Select or deselect **Replicate this attribute to the global catalog**.

Use Figure 3.9 to determine if you need to place a GC at your branch locations. Other factors to consider when determining the placement of GC in your environment include:

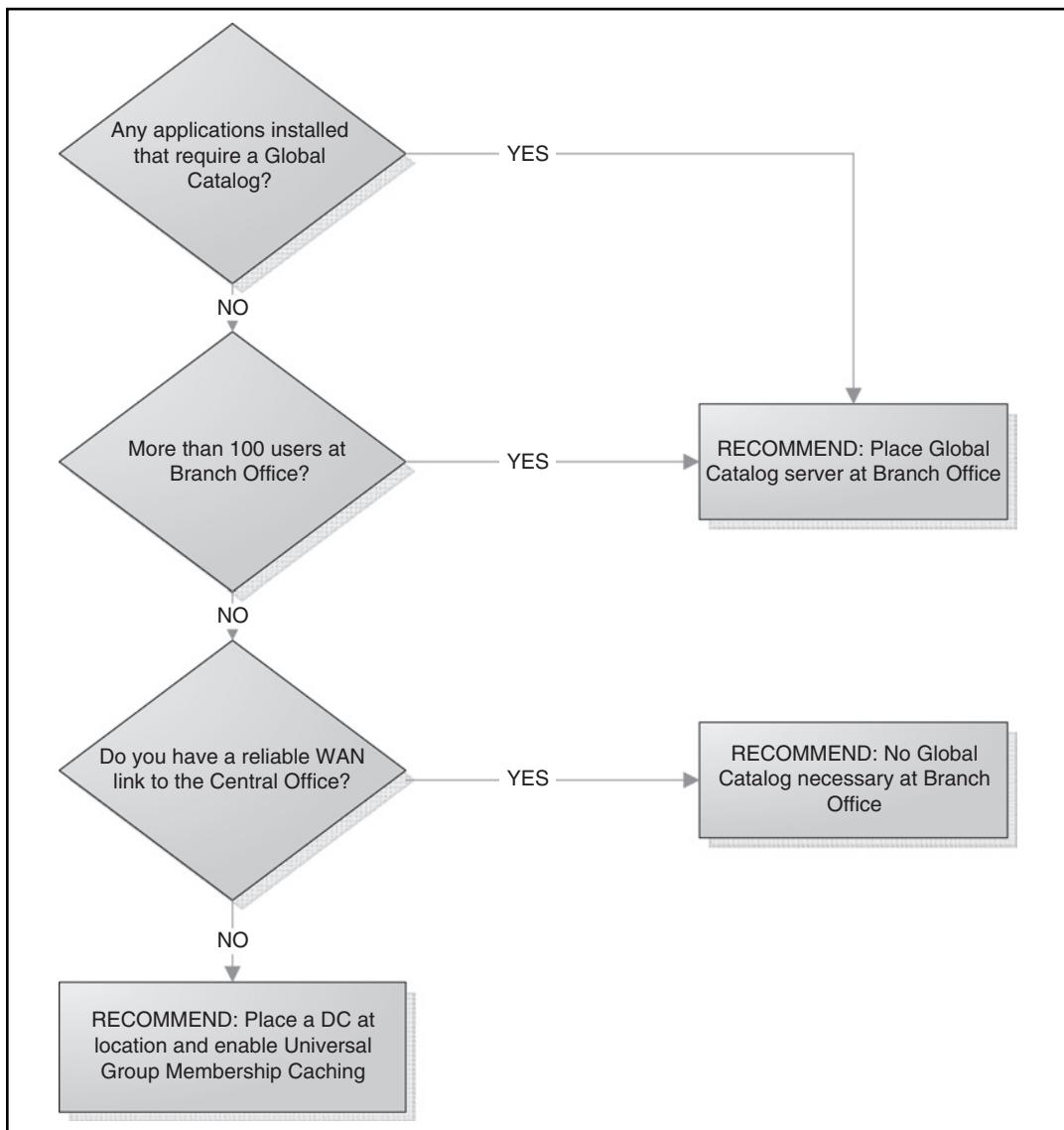
- **Application Requirements** Many applications, such as Exchange Server 2007, do not deliver acceptable response times over latent WAN links. Therefore, if you have an application that does not deliver acceptable response times, consider adding a GC to that location.
- **Large number of users** Typically speaking, if you have a domain controller in a location that has more than 100 users, consider making that DC a global catalog server.



TEST DAY TIP

Global catalog servers can successfully be installed on RODCs. However, there are certain applications, like Exchange Server 2003 and Exchange Server 2007 that will not use the RODC. Therefore, you must ensure that a writeable GC also exists and is always available.

- **Bandwidth** If you have highly available, reliable bandwidth, you do not need a GC at every location, even if there are applications that require it. These applications can use the WAN link as long as the response time is acceptable.
- **Universal Group Membership Caching** Windows Server 2003 forest function level and above give the ability for Universal Group membership caching. This means that a DC in a location without a GC, can query the GC over the WAN link as a user logs on, and then cache the Universal Group membership for future logons. To enable Universal Group membership caching:
 1. Open **Active Directory Sites and Services**.
 2. Expand **Sites**.
 3. Expand the site you wish to enable it on.
 4. Right-click **NTDS Settings** and then click **Properties**.
 5. Check **Enable Universal Group Membership Caching**.

Figure 3.9 Determine Whether to Add GC to a Branch Location

Earlier in this chapter we looked at the Active Directory logical topology; that is, designing the forest, trees, domains, and OUs. Active Directory Sites are part of the physical topology. The physical topology contains domain controllers and sites. Active Directory is physically installed on a DC. The DC physically resides in a network location. In this section we will look at designing the site topology and the replication topology.

Your site topology significantly affects the performance of your network and the ability of your users to access network resources. Creating your site design involves determining which of your branch locations will become an Active Directory site, creating the site link objects, site link bridge design, site object design, and subnet object design, and finally associating the subnet with the site. When considering the site design, you must have knowledge of the network bandwidth between all of your locations, the number of users, computers and other servers at each location, and what other services are running at each location. If you want to deploy domain controllers in a branch office that is distant from the central site, you can create a site object in AD DS to represent the branch office. When you create a new site object, you must connect the site with an existing site link. If you already have multiple sites, you may have to create an additional site link to connect the new site to an existing site. Remember, Active Directory Sites uses your existing routing queries and routing tables to route traffic from one location to another.

Use the following elements when deciding which locations will become sites:

- **Applications** Does the location include servers running applications that require a site to be created? Certain applications, like distributed file system (DFS) use site objects to locate the closest servers for the clients.
- **Domain Controllers** Create a site object for each location that has a domain controller. If you decide not to create a site object for a smaller location with a DC, create a subnet object for that location under the closest AD site.

Designing a replication topology is critical in ensuring all information is up-to-date with as little latency as possible. Latency is the time it takes a change made on one domain controller to be replicated to all domain controllers. Certain factors, such as the available network bandwidth greatly affect your replication topology. Other factors include the domain design, that is, which domain controllers replicate which Active Directory partition with which domain controllers; your site design, or how often replication is taking place; and the site link design, or what protocols are we using to replicate AD DS information, and whether or not are all site links are bridged.

Creating the Site Link Objects

Site links tell Active Directory domain controllers what the network is like between the physical locations. Creating site links is a way to influence your replication topology. When creating a new site, you must add that site to an existing site link. Therefore creating your site links first will help you “draw”

the picture of your physical network. If no other site links exist you can use the DEFAULTTIPSITELINK. The site link is defined by these six elements:

- **Name** The name should be descriptive. It is common to use a name that describes the sites it is linking. For example, if you were creating a link-to-link site that linked the Toronto and Boston locations, an appropriate name would be Toronto-Boston-Link.
- **Sites in this Site Link** AD DS uses the existing network to send data to other locations. This site link tells AD DS which DC to use when transferring data across the WAN link.
- **Transport Protocol** The two options here are IP and SMTP.
- **Cost** If there are two or more links linking the same sites together, the link with the lower cost will be used. A default cost of 100 is used when creating new site links.
- **Replicate Every** By default, the site link will open up for replication traffic every 180 minutes. This is configurable from as low as 15 minutes to as much as 10,080 minutes, or one week.
- **Schedule** If you have a period of time throughout the day where your WAN link is over taxed, you can ensure that no replication traffic happens during that time frame.

NOTE

SMTP replication will not be supported in future versions of AD DS; therefore, creating site link objects in the SMTP container is not recommended.

To create the site link object, your user account must meet one of the following:

- Enterprise Admin
- Domain Admin in the forest root domain
- Delegated the right to create site link objects

To create the site link object, log on as a user who is a member of at least one of these groups (or use Runas), and then do the following:

1. Open **Active Directory Sites and Services**.
2. Expand **Sites** and then expand **Inter-site Transports**.
3. Right-click the appropriate transport protocol.
4. Click **New site link**.
5. In the **Name** field, type a name for the site link.
6. In the **Sites not in this site link** section, **Add/Remove** sites as necessary, and then click **OK**.
7. Go to the **Properties** of the site to configure cost and other replication parameters.

Site Link Bridge Design

A site link bridge virtually connects two or more site links and enables traffic to flow between site links. Each site link in a bridge must have a site in common with another site link in the bridge. For example, in Figure 3.8, creating a site-link bridge between the “Montreal-Chicago Link” and the “Boston-Montreal Link” would allow all sites to be virtually linked together. Montreal is the site that each of these links has in common. To ensure that the link itself gets used, and not the site link bridge (when the link is available), the KCC takes the cost of each link and adds them together to determine the cost of the bridge. For example, if the Montreal-Chicago link has a cost of 100, and the Boston-Montreal link has a cost of 100, then the bridge has a cost of 200. Remember, the lower cost will win, provided it is available for domain controller traffic.

It is recommended that you keep all site-links bridged. However, there are certain situations where it is best to disable site link bridging:

- **Your IP network is not fully routed** If your IP network is not fully routed, then disable this feature, and then create site link bridges that model the actual routing behavior of your network. For example, in our example, if your network has no physical links between Chicago and Boston, do not enable bridging all site-links.
- **You wish to control the flow of replication in AD DS** By disabling all site link bridges and then manually creating and configuring site link bridges, all site links inside that bridge will route transitively, but will not route outside of the bridge.

- **Hub and Spoke Replication Model** In this model, all changes are made at the central location (or hub office) and then get pushed out to all other Domain Controllers. This way there are no changes made at branch office domain controllers, and no branch office domain controller will have another branch office's DC as a replication partner.

To disable automatic site link bridges:

1. Open **Active Directory Sites and Services**.
2. Expand **Sites | Inter-Site Transports**.
3. Select the transport container (IP).
4. Right-click the transport protocol and then select **Properties**.
5. Deselect **Bridge all site links**.

Creating the Site Objects

For each location that you have decided to create a site, you need to create the site object in AD DS. To create the site object, your user account must meet any one of the following:

- Enterprise Admins group
- Domain Admins group in the forest root domain
- Delegated the right to create site objects

To create the site objects, log on as a user who is a member of at least one of these groups (or use Runas), and then do the following:

1. Open **Active Directory Sites and Services**.
2. Right-click **Sites** and then click **New Site**.
3. Type a name for the site.
4. In the **Link Name** field, click an existing site link and then click **OK**.

TEST DAY TIP

It is recommended that you use proper DNS names when naming your site. That is, do not use certain characters or spaces. Otherwise, your site will only be accessible wherever you have a Microsoft DNS Server.

Creating the Subnet Objects

For every IP subnet and subnet mask associated with each location, whether IPv4 or IPv6, plan to create subnet objects in AD DS. To create the Subnet Objects in AD DS, your user account must meet one of the following:

- Enterprise Admins group
- Domain Admins group in the forest root domain
- Delegated the right to create subnet objects

The reason we create subnet objects in Active Directory is to let applications and other services “know” where we are in relation to the domain controllers. For example, when we log on, our client computer queries DNS for a domain controller in our site for authentication. Based on our IP address and the IP subnets created in Active Directory, DNS is able to point us to the appropriate DC.

To create subnet objects, log on as a user who is in one of these groups (or use the Runas command) and then do the following:

1. Open **Active Directory Sites and Services**.
2. Expand **Sites** and then click **Subnets**.
3. Right-click **Subnets** and then click **New Subnet**.
4. In the **Prefix** field, type the subnet address in CIDR notation (192.168.1.0/24).
5. In the **Select a site object for this prefix** field, select the site and then click **OK**.
6. To modify any of the properties of the subnet object, right-click the subnet object and then click **Properties**.

Printer and Location Policies

Most standard users on your network will not know the names of the printers on your network. And even if they did, they may not know all of the features the printer has installed, such as printing in color, or stapling. For this reason, Windows Server 2008 comes with a way for the users to search Active Directory for a printer near them, searching by name, location, feature, and so on.

This feature is most effective when carefully planning your subnet object strategy. In Active Directory Sites and Services, we have already shown you how to create the subnet objects, and associate the subnet with the site object. Enabling a printer’s location is a multi-step process:

1. Modify the subnet object properties to include the Location attribute.
2. Create or modify a group policy object.
3. Ensure all printers have the Location attribute set in Active Directory.
4. Ensure the users can browse Active Directory.

After you have created the subnet object following the steps above, you must modify the subnet to include the Location attribute. This attribute can be broken into sections to give the most descriptive location (USA/Ma/Boston/Lincoln Street/floor5), or can be less descriptive (Boston). Check with the network team to ensure that the subnet is only on Floor 5 in my previous example, or if the subnet spans multiple offices or floors, the subnet object in Active Directory should not go so deep.

To add the subnet object's location attribute, open Active Directory Sites and Services and follow these easy steps:

1. Expand **Sites** and then expand **Subnets**.
2. Right-click the subnet that you wish to modify, and then click **Properties**.
3. Click the **Location** tab.
4. In the **Location** field, type in the location using the example above and then click **OK**.

TEST DAY TIP

If the Browse button is active, you may click it and browse for the location. It will be dim until the group policy has been enabled. We will cover that in the next section.

The next step, once the subnet object has been created and its Location attribute has been added, is to create or modify an existing group policy object (GPO). For information on managing and designing group policy objects, see Chapter 4. But for now, we will create a new GPO, called printer location policy, and link it directly to the domain. To create the GPO, follow these steps:

1. Open the **Group Policy Management** console.
2. Expand **Group Policy Management | Forest: your forest | Domains | Your domain**.

3. Right-click the *domain name* and then click **Create a GPO** in this domain, and **Link** it here.
4. In the **Name** field, type **Printer Location Policy** and then click **OK**.
5. Right-click **Printer Location Policy** and then click **Edit**.
6. Expand to **Computer Configuration | Policies | Administrative Templates | Printers**.
7. Right-click **Pre-populate printer search location text** and then click **Properties**.
8. Click **Enabled** and then click **OK**.

Once this has been enabled, and the group policy is refreshed on the print servers, during the installation of a new printer, make sure you browse for the printer's location in the Add Printer Wizard.

By default, all printers installed in an Active Directory environment are published in Active Directory once they are shared. To ensure the shared printer is published in Active Directory:

1. Open **Active Directory Users and Computers**.
2. From the **View** menu, click **Users, Contacts, Groups, and Computers** as containers.
3. Expand the console tree until you can click on the server object on which the printer is installed.
4. In the **Details** pane, right-click the printer object and then click **Properties**.
5. Ensure the **Location** field is filled in, otherwise type it in this field.

NOTE

You can get even more precise here if you wish. For example, you can add Copy Room, or Sales Office to the end of the Location attribute.

Active Directory reads from the driver how fast this printer prints, whether it staples, or prints color, and so on and automatically fills in that information.

Continue these steps until all of the printers have the location attribute supplied. Remember, if you do this early in design and implementation stages, you can accomplish this while adding the printers, instead of after-the-fact.

By default, all users have read access to Active Directory, and therefore can search for things like printers or other users. However, you do not want to give your users the Active Directory console in which to do the search. When installing printers, while running the Add Printer Wizard, the user can specify to search the directory, and this will search Active Directory for all shared printers. However, if the user is looking for a specific printer in a specific location, or one that has certain features, there is a better way. The following steps will create a shortcut on the desktop that will allow the user to search Active Directory for printers (and other objects) and then install the printers on their workstation.

NOTE

Do not expect to see this on the exam. This is for informational purposes only.

1. Right-click anywhere on the **Desktop** and then click **New | Shortcut**.
2. In the **Type the location of the item** field, type **rundll32 dsquery, OpenQueryWindow** and then press **Next**.
3. In the **Name** field, give a descriptive name for this shortcut, such as **Search for Printers**, and then click **Finish**.
4. Double-click the shortcut and then in the **Find** field, select **Printers** (the Location attribute will be filled in by DNS querying Active Directory for the location of your IP subnet).
5. Either click **Find Now** or click the **Features** tab to add additional features, such as **Can print double-sided** or **Can staple** and then click **Find Now**.
6. Right-click the printer and then click **Connect**.

Remember the magic here is the subnet object in Active Directory Sites and Services having the proper Location attribute filled in. Once that has been filled in, DNS will query Active Directory for the printer closest to you based on your computer's IP address and the Location attribute that has been set in Active Directory Sites and Services.

Designing an Active Directory Administrative Model

Just like in other businesses, the administrative model of Active Directory Domain Services (AD DS) shows who *makes* the decisions and who *follows* those decisions. We can clearly see this in an organizational chart. We can see that the person at the top of the chart makes the decisions, and those on the bottom of the chart follow those decisions. However, there are usually several layers in between, and those people in the middle layers make some rules, that others below them have to follow, and follow some rules that those above them have made. There is no organizational chart that will be the same for every business. Likewise, no two Active Directory forests will look the same or be managed the same. Therefore, understanding the administrative model is imperative to designing the best Active Directory for *your* requirements.

Before installing AD DS, you should know how the company is being managed. Does it have any branch offices? Are there managers in those branch offices? How much control do the department managers have over their employees? Are the department managers allowed to hire their own employees and then create accounts for those employees, or are the accounts created and managed by another team? These are all questions that would need to be answered, as designing AD DS can follow these same elements. The elements that will make up the administrative model design are delegation, group strategy, and compliance strategy. The different models we can design in AD include centralized, distributed, or a hybrid model.

In the centralized model, a single administrator or group of administrators makes all of the IT decisions in the forest. Typically this would be in a single-domain forest. Keep in mind that even in this model, you can still delegate some responsibilities, but ultimately it is this group or individual that is responsible to make sure the job gets done and gets done correctly.

It is not uncommon to see this type of administrative model where certain tasks are delegated at the organizational unit (OU) level, such as unlocking user accounts, or changing passwords, and other tasks are delegated at the domain level, like creating and linking group policy objects. In other words, any task that may affect multiple users will be done at the domain level, and managed by the Domain Admins group. Other tasks that only affect a small group of users may be delegated at the OU level.

In a Distributed model, a single individual, or a single group of administrators is not ultimately responsible for all of the administrative IT tasks throughout the enterprise. The way you implement this design varies on the requirements of the organization. For example, a single forest with multiple domains, and therefore multiple Domain Admins groups, would be considered a distributed model. An organization that decides

multiple forests are best would also be a distributed model. In this model, there are several teams responsible to make sure the administrative IT tasks are getting done and, depending in the task, which group will take ultimate responsibility.

A key factor in determining which model is best for your organization is the level of delegation you are willing to allow. In other words, even in a single domain forest, if the domain administrator decides to delegate group policy creation and linking, he has created a distributed IT infrastructure.

Delegation

Delegating administrative control is the process of assigning permissions to a user or group of users to perform administrative tasks. This can be done by modifying access control lists (ACLs) on Active Directory objects, or by adding users to groups which in turn gives them administrative rights, for example the Group Policy Creator Owners group which gives users the ability to create group policy objects anywhere in the domain. It is important to note, however, that membership in this group is not enough to also link the group policy objects. Members can only create them.

As we have learned earlier in the chapter, organizational units (OUs) are a piece of the Active Directory logical structure. This means that it makes no difference which OU a user or other security principal is in, he can still access network resources or be authenticated by a domain controller.

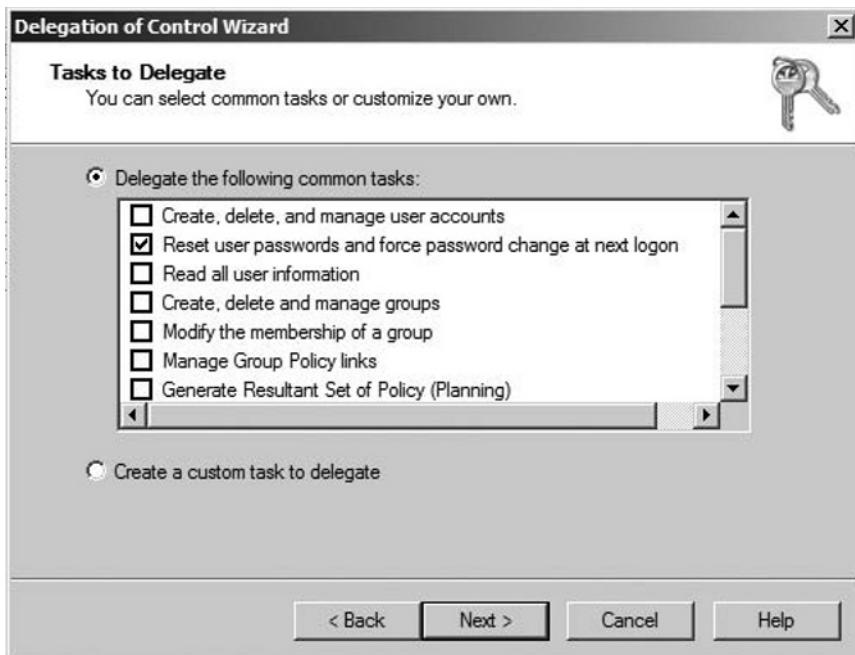
Then why use OUs? One of the biggest reasons for putting a user into one OU over another is delegation. Delegation at the OU level means that whatever task is delegated here can be done for all security principals within the OU. In other words, let's say we have a Sales OU and all of the members of the sales team have their user objects placed inside of this OU. We can delegate the ability to change users' passwords for all user objects in this OU to the sales manager. If those user objects were scattered around Active Directory, delegation would not be so easy.

Using this example, let's say we have a sales manager who is a member of the Global-Sales OU Admin Security group. We also have a Sales OU, in which we place all of the sales users. Use the following steps to delegate the ability to change password:

1. Open **Active Directory Users and Computers** as a member of the Domain Admins group (it is recommended that you use Runas).
2. Right-click the **Sales OU** and then select **Delegate Control**.
3. In the **Delegation of Control Wizard**, click **Next**.
4. On the **Users or Groups** page, click **Add**.
5. In the **Select Users, Computers, or Groups** dialog box, type **Global-Sales OU Admins** and then click **OK**.

6. On the **Users or Groups** page, click **Next**.
7. In the **Tasks to Delegate** dialog box, select **Reset user password and force password change at next logon** and then click **Next**.
8. On the **Completing the Delegation of Control Wizard** page click **Finish** (see Figure 3.10).

Figure 3.10 Delegation of Control Wizard



Group Strategy

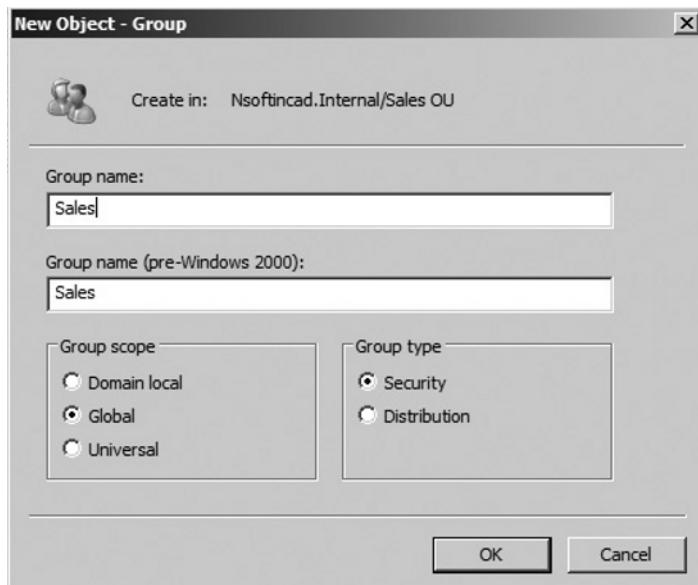
A group is a collection of users, contacts, computers or other groups that can be managed as a single unit. Upon installation, Windows Server 2008 comes with several default groups. It also comes with the ability to add more groups, as your organization or administration sees fit. Groups are not the same as Organizational Units. OUs contain the user, contact, and computer and group accounts for administrative purposes. But you cannot assign permissions to an OU. Groups contain these objects for the purpose of assigning permissions to a large number of security personnel, or for sending email to a large number of users, instead of adding each one at a time. As we discuss groups, it will be important to understand the different types of groups and the scope of each group. How you use groups will affect who can access your network resources or who has permission to modify an Active Directory object.

Group types define whether the group will be able to be used as a security principal, that is whether or not it can be used to assign permissions, also known as a security group, or if it can only be used as an email distribution group, known just as a distribution group. Use the following considerations when determining which type of group to create:

- **Distribution Group** Can only be used for email distribution. You must use an email program such as Microsoft Exchange or Windows Mail to send the email. These groups are not security-enabled. This means that if you need to assign resource permission to a shared resource, or wish to delegate control to an OU, you cannot use this type of group.
- **Security Group** This type of group can be used as an email distribution group or as a security principal. Membership in this group gives the user all of the rights and permissions that have been assigned to the group. For example, a user who has been placed into the Group Policy Creator Owners group has the ability to create group policy objects (GPO).

The scope of the group determines the extent of which this group can be used within the domain or forest. Regardless of the group type, it will still fall into one of the following three scopes: domain local, global or universal. When you create a new group in AD DS, it will default to being a global security group, unless you specifically click a different radio button. See Figure 3.11.

Figure 3.11 Scopes and Types of Groups Available. The Default Is Global Security.



The recommended practice is to assign resource access permissions to domain local groups (DLGs). DLGs can contain members from other domains, provided the appropriate trust relationship exists, but can only be assigned resource access to resources in its own domain. See Table 3.4 for a summary table of the group membership rules, and visibility of the group.

Global groups can contain members only of the domain in which the global group is defined, but are visible in all other trusted domains. Visibility means that you can add global groups in one domain to DLGs in another domain.

As we have learned, domain local groups can contain members from all domains, but are visible only in the domain in which it is defined. Global groups are visible in all domains, but can contain members only from the domain in which it is defined. The groups with a universal scope can contain members from all trusted domains, and are visible in all trusted domains. The best of both worlds.

When deciding to use universal groups, use care in designing the membership rules. Because universal groups are a way of consolidating multiple groups from multiple domains in your forest, the membership in a universal group is replicated as part of global catalog replication. This means that membership changes must replicate as well. If you use Global groups as the members, then changes to the global group membership will not trigger a replication of the global catalog. However, adding individual users to the universal group will trigger a replication. See Table 3.4 for a summary of membership rules and visibility of all groups.

Table 3.4 Group Membership Rules and Visibility

| Group Scope | May Contain as Members | Visibility |
|--------------|---|------------------------|
| Domain Local | Users, contacts, computers Domain Local groups Global groups Universal groups From ANY domain | Its own domain only |
| Global | Users, contacts, computers Global groups From OWN domain only | In ALL Trusted domains |

Continued

Table 3.4 Continued. Group Membership Rules and Visibility

| Group Scope | May Contain as Members | Visibility |
|--------------------|--|------------------------|
| Universal | Users, contacts, computers Global groups Universal groups From ANY domain | In ALL Trusted domains |

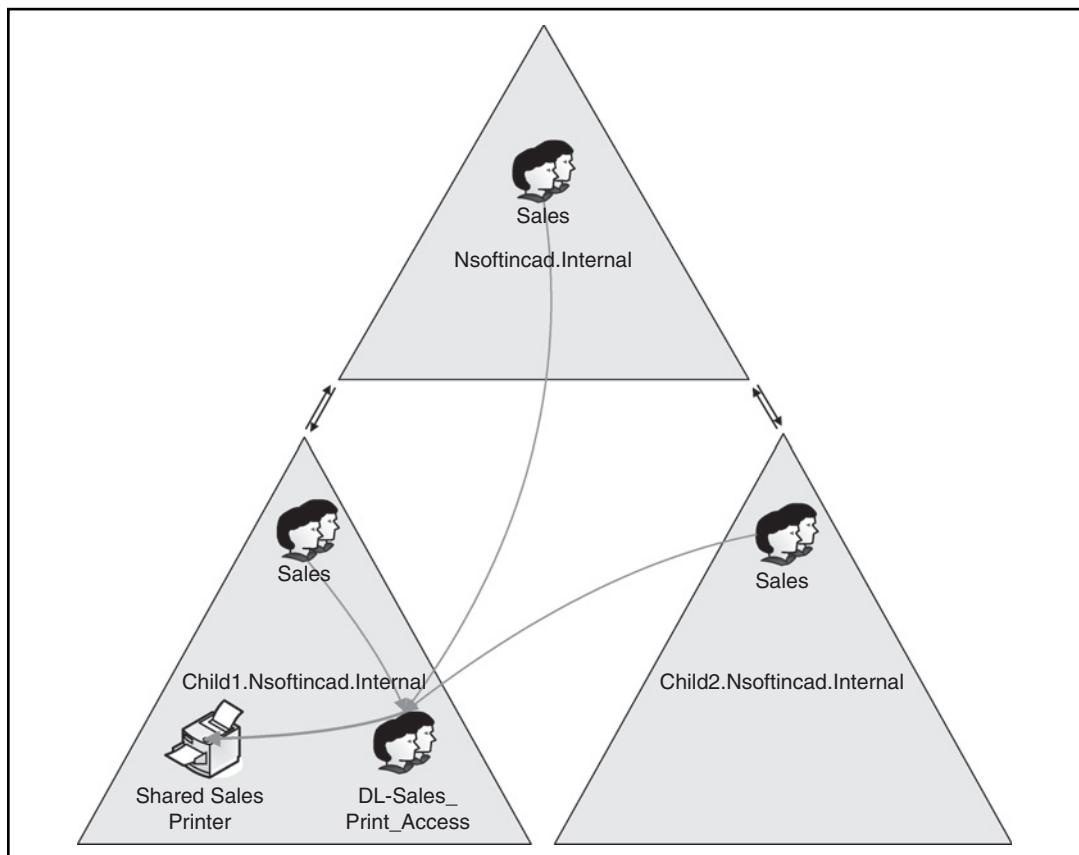
Special identity groups are default groups in Windows Server 2008 that cannot be created, and you cannot add or remove members from. Members are added and removed through normal network access. An example of this type of group is the Everyone group. Everyone, including users and guests from the local domain and all trusted domains, are automatically added to the Everyone group at logon. Although Special identity groups can be assigned rights and resource access permissions, group scopes do not apply to these groups. Also, group membership is automatic and cannot be modified or even viewed. Other Special identity groups include:

- **Anonymous logon** This group represents users and services that access a computer and its resources through the network without using an account name, password, or domain name. In Windows Server 2008, this group is *not* a member of the Everyone group.
- **Network** This group represents users who are currently accessing a resource over the network, as opposed to users who access a resource by logging on locally at the computer where the resource is located.
- **Interactive** This group represents all users who are currently logged on to a particular computer and who are accessing a given resource that is located on that computer, as opposed to users who access the resource over the network. This includes users who use an RDP (remote desktop) session to access a server, such as a terminal server.

The recommended practice for using groups in your organization is to create user accounts, add those accounts to global groups, add the global groups to domain local groups, and then assign resource access permissions to the domain local group. This is known as A-G-DL-P. Let's use the following example, which is shown in Figure 3.12. If we have a forest with three domains, each with a global security group for their sales department users, and each need access to a shared network printer located in Child1, you would use the following steps to grant the required access:

1. Create the user accounts for each member of the sales department team in each domain.
2. Create a global security group in each domain, and then add the appropriate user accounts to the global security group.
3. Create a domain local security group in Child1 and add the global sales security group from each domain into this domain local group.
4. Assign permissions to use the printer to the domain local security group.

Figure 3.12 Recommended Group Strategy (A-G-DL-P)



Compliance Auditing

Today, there are many regulatory boards ensuring companies practice sensible business practices. Your company should be no different. With regard to Active

Directory, creating a user account or changing a user's password could have serious security implications. As well as several other administrative tasks that can be accomplished.

Earlier in this chapter we discussed the new auditing feature of Windows Server 2008 Active Directory Domain Services. This new feature is important because the ability to identify how object attributes change makes the event logs more useful as a tracking mechanism for changes that occur over the lifetime of an object. Table 3.5 explains how the events get logged in the EventViewer's Security Log and Figure 3.13 shows an example of the Security log.

Table 3.5 AD DS Auditing Events

| Event ID | Type of Event | Event Description |
|----------|---------------|--|
| 5136 | Modify | Successful modification to an attribute in AD DS |
| 5137 | Create | New object is created in AD DS |
| 5138 | Undelete | Object is undeleted in AD DS |
| 5139 | Move | Object is moved in AD DS |

Figure 3.13 Security Log Event Upon Creating New User



This new auditing feature is implemented by using the following:

- Global audit policy
- SACL
- Schema

Global Audit Policy

In Windows Server 2008, this global audit policy is enabled by default, as are the four subcategories. It is enabled under the default domain controllers policy (Computer Configuration | Local Policies | Audit Policy) and is set to only audit success events. Because it is set by default, so is the subcategory Directory Service Changes, which will track modifying this policy. In other words, if one of the other administrators turns off Directory Services Auditing, that event will get audited and recorded.

With the new audit subcategory Directory Service Changes, successful changes are now tracked, as well as their previous and current values. Settings for both Directory Service Access and Directory Service Changes subcategories are stored in the Local Security Authority (LSA) database, and can be queried using the new LSA application programming interfaces (APIs). These subcategories are independent of each other; you can disable Directory Service Access and still track Directory Service Changes, and vice versa.

There is no Windows interface that will allow you to make these changes, however. The command line tool auditpol.exe will allow you to view the policies, and enable or disable them. To enable the Directory Service Changes subcategory, for example, open a command prompt with elevated rights, type the following, and then press **Enter**:

auditpol.exe /set /subcategory:“directory service changes” /successenable

SACL

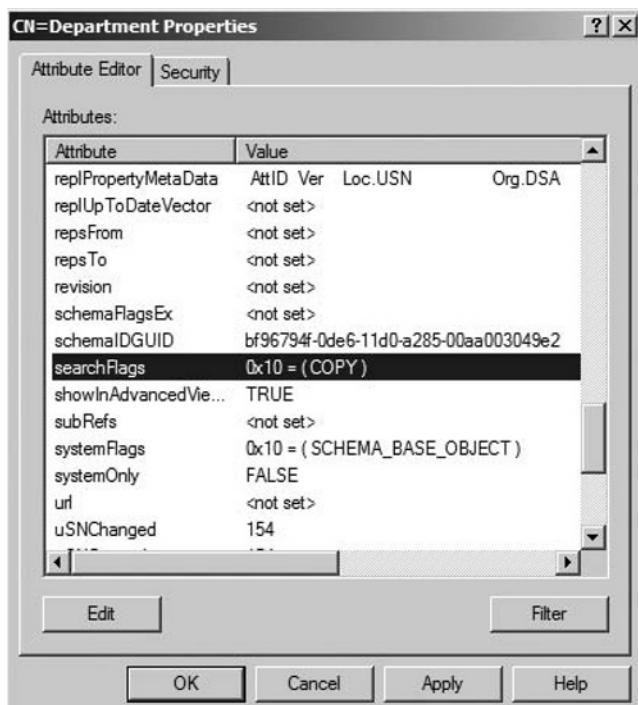
Security Access Control Lists (SACLs) are the ultimate authority in determining whether an event will be audited or not. The content of the SACL is controlled by the security administrators for the local system. Security administrators are users who have been assigned the **Manage Auditing and Security Log** (*SeSecurityPrivilege*) privilege. By default, this privilege is assigned to the built-in Administrators group and can be modified through a local security policy by modifying **Computer Configuration | Windows Settings | Local Policies | User Rights Assignments**.

If there is no access control entry (ACE) in the SACL requiring any attribute modifications to be audited and logged, even if the **Directory Service Changes** subcategory is enabled, no change auditing events are logged. For example, if there is no ACE in an SACL requiring write property access on the Department attribute of a user object to be audited, no auditing events are generated when the Department attribute is modified, even if the subcategory **Directory Service Changes** is enabled.

Schema

Because it is possible that a large number of events will be generated, and so that these events do not become unmanageable, there is a new schema attribute that you can use to create exceptions to what gets audited, and what does not. The **searchFlags** attribute determines what gets replicated to the global catalog, what attributes get copied when copying an object, and so on. If you wish to audit all changes to user objects, except for a couple of attributes, the best way to do this is with the ADSI Edit MMC snap-in. Set the attribute value to 256 (bit 9). When the attribute is set to 256, no auditing will take place on that attribute. Figure 3.14 displays ADSI edit, bound to Schema, setting the Department attribute to 256 from the default value.

Figure 3.14 ADSI Edit MMC Snap-in



Summary of Exam Objectives

Regardless of how long you have worked with Active Directory, proper planning needs to take place before introducing Windows Server 2008 into your environment. There have been many new features, advanced features, that are now included with AD DS, so designing your strategy is essential to a successful deployment.

Windows Server 2008 Active Directory has been broken down into several components. These are:

- AD Domain Services (AD DS)
- AD Lightweight Directory Service (AD LDS)
- AD Certificate Services (AD CS)
- AD Rights Management Services (AD RMS)
- AD Federation Services (AD FS)

In this chapter we concentrated on designing the AD DS infrastructure. First, we discussed some of the improvements to AD DS, such as RODC and Restartable Active Directory. We also saw in this section Fine-grained Password policies. These policies make it possible to set a password or lockout policy on a group of users within the domain. Remember, this is new. In previous versions of Windows, if we had different groups of users that needed a different set of password policies, we had to separate the group into different domains. This required more hardware, more administration, and so on.

Next we discussed some of the factors to consider when designing your forest and domains. Some of the factors are your timelines, budgets, or the namespaces you wish to use. In this section we discussed that because one business unit in the organization may wish to have AD DS up and running earlier than the others, a separate forest may be required for this business unit. We also said that planning can take place to ensure that when the other areas are ready to install AD DS, they might be able to simply join the forest, as opposed to creating their own. Joining the forest would ease the administration of this company.

Then we talked about the Active Directory logical structure versus the physical structure. The logical structure includes forests, trees, domain, and OUs or organizational units. We called them logical pieces because a user account may exist in any OU, in any domain in the forest; but a user account with the appropriate permissions can access any folder on any member server in the entire forest. The physical

structure is the Domain Controller (DC) itself and the sites, or physical network location, that the DC is placed in. We can connect sites together with site links, and can manage replication by managing these site links. We also said that site link bridges, which are enabled by default, may be disabled to allow you, the enterprise administrator, to determine which DCs replicate with which DCs. Subnet objects came up as we talked about sites, as they are required to tell DNS and other directory-enabled applications, where the DC is located in relation to the other services needing it. For example, when a user clicks a DFS link to open a shared folder on the network, DFS will use the user's IP address and query AD for the DFS link closest to the user, based on ADs knowledge of the network and subnets.

After that we talked about installing the forest root domain, the operations masters, and the forest and domain function levels. Remember to plan the function levels carefully as they cannot be reversed, and raising to a function level that is not yet supported by all of the DCs may affect the functionality of the network.

Finally we looked at designing the administrative model of Active Directory. In this section we saw how to delegate administrative control, and we looked at the different types and scopes of AD groups, and Active Directory auditing.

All of this planning seems like the design of Active Directory will take months. In most cases, proper planning will take months. This is not an easy task. The network health, the users' happiness, and the organization's growth all depend on a proper design. And do not just design for the present. If you have a five-year business plan, take it into consideration when planning AD. If you will need additional domains or sites five years from now, proper planning today can make the growth tomorrow easier.

Exam Objectives Fast Track

Designing Active Directory Forests and Domains

- In previous versions of Active Directory, if you needed to set different password or lockout policies for different groups of users, you needed to create a multi-domain environment. Windows Server 2008 fine-grained password policies allow you to create different password or lockout policies based on security group membership. Remember, you use ADSI Edit to create and apply fine-grained password policies.
- If your company has different schema requirements, you will need to design a multi-forest environment, as Active Directory allows only a single schema per forest.

- Create your OU design for delegating administrative control and for group policy linking. An object can be in only one OU, so ensure the OU that object has been placed in will not compromise security.
- Forest and domain function levels tell Active Directory what features will and will not be available. Set the domain function level at the highest available level; that is, the level of your lowest domain controller. Once the domain function levels are set, set the forest function levels to the level of your lowest domain. Once these levels are raised they cannot be lowered, and you can not reverse the action of raising the function level. Also, if you set the function level higher than your lowest domain controller, then you will lose functionality.

Active Directory Topology

- Operations masters are also known as flexible single master operations, or FSMO roles. There are five operations master roles. The schema master and the domain naming master are forest-wide. This means that there is one schema master and one domain naming master per forest. The PDC emulator, the RID master, and the infrastructure master are all domain-wide. This means that there is one in each of the domains in the Active Directory forest.
- Site links connect the Active Directory Sites for replication, query, and FSMO traffic. The option to bridge all site links is enabled by default. Only disable this if your network is not fully routed, or if you wish to set your own replication objects in Active Directory Sites and Services. Disabling this could cause a domain controller in one site to not find a domain controller in another site for because of password changes, or to replenish a depleted RID pool.
- Subnet objects tell Active Directory where the domain controllers are in relation to the other servers and workstations on the network. By defining subnet objects and location attributes, Active Directory builds a logical “map” of the physical network. By filling in the Location attribute, and setting the group policy **Prepopulate printer search location text**, users can browse Active Directory for printers close to them and, based on their subnet, DNS, and other directory-enabled services, can direct the client to the server or service closest to them.

Designing an Active Directory Model

- Active Directory groups can be used to assign permissions to objects or to send email to multiple users at one time. The scope of the group that you use will determine which users may be placed into them. The type of the group determines whether or not this group can be used for assigning permissions to resources or for email distribution only. Security groups are used for ACLs and SACLs whereas distribution groups are used for email distribution lists. The Global Security group is the default group, and can contain members from its own domain only, but can also be added to groups in each trusted domain.
- SACLs, or system access control lists, are used for auditing. By default, Active Directory domain controllers audit changes made to active directory objects. In previous versions, only a change was logged. In Windows Server 2008, the previous and current values also are logged. That is because of the subcategories of Active Directory auditing. These subcategories are all enabled by default, but can be disabled by using an auditpol.exe command line.
- If you wish to audit Active Directory changes, except for minor changes like Description or Comment sections, use ADSI Edit to modify the searchFlags attribute of the attribute you do not want to audit.

Exam Objectives

Frequently Asked Questions

Q: All of this planning seems like a lot of work. I just have a small company with a single domain. Do I still need to plan?

A: Yes. I know it seems like a lot of work. But proper planning is necessary. You need to know what to expect, you need to have a fallback plan, and you need to be prepared if you ever decide to take your company to the next level.

Q: I have been working with Windows Server systems since Windows NT 4.0. I have been using Active Directory since Windows 2000 and currently use Windows Server 2003 Active Directory. Why do I still have to plan?

A: There have been many changes since the days of NT 4.0, that's for sure! And you have been keeping up with the changes. But you still need to plan whether you are going to do an in-place upgrade or a clean installation of Windows Server 2008. You need to be prepared for the RODC and AD RMS, if you decide to use them. Planning will help you make those decisions.

Q: We still use Windows NT 4.0, and know we will be doing a clean installation and creating all of our users and groups from scratch. Do we still need to assess our current environment?

A: Yes. (Do you see a theme here?) You have decided not to use your current servers and technology, but still need to be aware of your business units, any legal compliance issues with your industry, security, the namespace that you will use, and so on.

Q: When we upgraded from Windows 2000 Active Directory to Windows Server 2003 we did all this planning. Can we go back to that assessment instead of reassessing our environment?

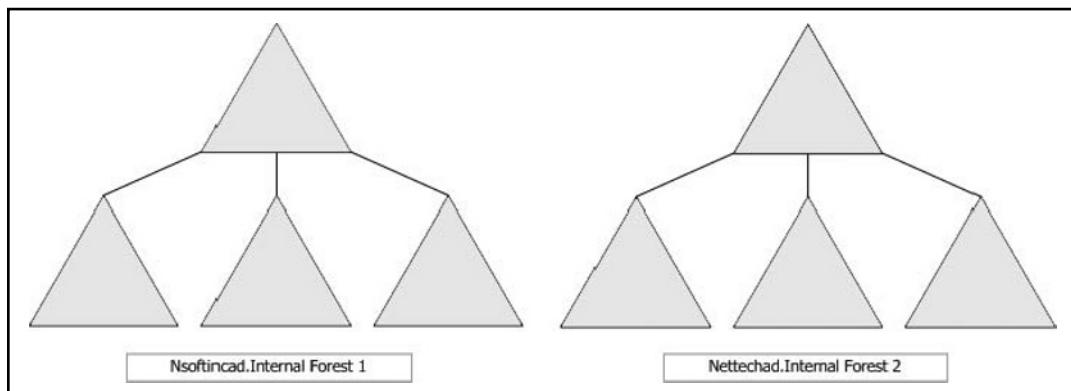
A: More than likely things have changed since then. When you upgraded from Windows 2000 to Windows Server 2003, you upgraded to many nice new features of Active Directory. Now there are even more. There have been many changes since Windows 2000, so the assessment you did then, even though it was thorough, will not answer all of the questions that now need to be answered. Today's Active Directory gives us fine-grained password policies, RODCs, and the ability to take a snapshot of Active Directory at different times. Since these features were not available previously, your assessment did not take them into consideration.

Self Test

1. You are planning a Windows Server 2008 Active Directory infrastructure. You have a single location and there is a limited budget. During your planning process, you have determined that the members of the Domain Administrators group should have a password policy that states passwords must be changed every 24 days, and the rest of your users must change their passwords every 42 days, except for members of the Enterprise Admins group. These users must change their passwords every 14 days. What is the best way to accomplish this without going over your budget, and keeping administration to a minimum?
 - A. Create a single forest with three domains. In the forest root domain set a domain-wide password policy that states users must change their passwords every 14 days. Ensure all enterprise-wide administrators are placed into the Enterprise Admins group in the forest root domain. Create two child domains specifying the appropriate password policy in each domain.
 - B. Create a single forest with two domains. In the forest root domain set a domain-wide password policy that states users must change their passwords every 14 days. Place all administrative users into the Enterprise Admins group in this domain, including those specified as Domain Admins. In the child domain, create a domain-wide password policy with the appropriate attributes and ensure only non-administrative users log on as users from this domain.
 - C. Create a single-domain forest. Place all enterprise-wide users into the Enterprise Admins group, all domain administrators into the Domain Admins group, and all other users into the Users group. Create three password security objects (PSOs) with the appropriate attribute values set and deploy them to the appropriate security groups.
 - D. Create a single-domain forest. Create three organizational units (OU), one for enterprise-wide administrators, one for domain administrators, and one for the rest of your users. Place all enterprise-wide users into the Enterprise Admins OU, all domain administrators into the Domain Admins OU, and all other users into the Users OU. Create three password security objects (PSOs) with the appropriate attribute values set and link them to the appropriate OU.

2. You are assessing the design of an Active Directory infrastructure for a company that has several business units. For legal reasons, these business units must remain separate entities each managing its own Active Directory infrastructure. What would be the best design for this company, keeping their requirements in mind when creating the design?
 - A. Create a single-domain forest, and place each business unit into its own organizational unit (OU).
 - B. Create a single forest, and place each business unit into its own tree.
 - C. Create a single forest and place each business unit into its own domain.
 - D. Create a separate forest for each business unit.
3. You have been hired to assess the installation of a Windows Server 2008 forest for a large company. The company will have nine business units, each using their own IT staff. For security and regulatory reasons, one of these business units must remain separate from the rest of the company. The other eight business units will need to have the ability to make their shared resources available to each other, in the need that a user from one business unit needs access to resources from another business unit. The other eight business units would also like to share a common global catalog (GC) database. Domain controllers from each business unit should not replicate user information to domain controllers outside of the business unit. How should you design Active Directory to meet the needs of this organization, with the least amount of administrative effort?
 - A. Create two forests. In one forest place the eight business units, each in their own domain. In the other forest place the other business unit. As the resource access needs arise, create Domain Local groups in the appropriate domain for giving permissions to the resources.
 - B. Create nine forests. For the eight business units that would like to allow access to each other's users to their resources, set up cross forest trusts. Set up connection objects in Active Directory Sites and Services to allow the GC in each forest to replicate with each other.
 - C. Create one forest. For the business unit that would like to remain separate, create its own tree. Place the other eight business units in the same tree of the forest.
 - D. Create two forests. In one forest place the eight business units, each into their own Organizational Unit (OU). Place all user, computer and domain controller objects into the appropriate OU. In the other forest, place the other business unit.

4. You have been asked to help design the Active Directory infrastructure for a large organization. One department in this company will be installing an application that will make several modifications to the Active Directory schema. The rest of the company must not see those schema modifications. However, there will be some resources that will be shared by all departments. What is the best way to design this company so that only the department using the application can see the schema modifications?
 - A. Create a single forest with two trees. In the first tree, place all of the departments that do not need this specialized application into their own domains. In the second tree, place the department that uses this specialized application into its own domain. Transfer the schema master to the domain controller in the second tree and make the modifications to the schema.
 - B. Create a single forest with two trees. In first tree, place the one department that needs the application. Modify the schema on the schema master. Then create the other tree and add the rest of the departments to the domain in the second tree.
 - C. Create two forests each with a single domain. In the first forest add the department that uses the specialized application and modify the schema. In the second forest place the rest of the departments. Create a cross-forest trust between the two forests.
 - D. Create two forests each with a single domain. In the first forest add the department that uses the specialized application and modify the schema. In the second forest place the rest of the departments. Ensure **Bridge all site links** has been enabled for both forests.
5. You have designed the Active Directory infrastructure for a company that has two forests, each with four domains (as shown in Figure 3.15). You are doing an inventory of all of the domain controllers and the operations master tokens they hold. How many of each should you expect to find?

Figure 3.15 Active Directory Infrastructure for a Company with Two Forests

- A. 2 Schema, 2 Domain Naming, 8 Infrastructure Master, 8 PDC Emulator, 8 RID Master
- B. 8 Schema, 8 Domain Naming, 8 Infrastructure Master, 8 PDC Emulator, 8 RID Master
- C. 2 Schema, 2 Domain Naming, 8 Infrastructure Master, 8 PDC Emulator, 8 RID Master
- D. 8 Schema, 8 Domain Naming, 2 Infrastructure Master, 2 PDC Emulator, 2 RID Master
- 6. You have been asked to assist in the upgrade of a single-domain forest from Windows Server 2003 to Windows Server 2008. Currently all DCs in all domains run Windows Server 2003. You decide to upgrade the DCs to Windows Server 2008 as an in-place upgrade. However, the company is running an application that must reside on DC running Windows Server 2003, so you decide that it would be best to keep that DC running Windows Server 2003 until the application vendor upgrades the application. What is the best way to upgrade this forest, while keeping the application running?
 - A. Upgrade the first DC to Windows Server 2008. Make sure the forest function level and domain function level remain at Windows Server 2003. When the application gets upgraded, upgrade the final domain controller and then raise the forest function level to Windows Server 2008.
 - B. Upgrade the first DC to Windows Server 2008. Raise the forest function level to Windows Server 2008 but keep the domain function level at Windows Server 2003. When the application gets upgraded, raise the domain function level to Windows Server 2008.

- C. Uninstall the application. Upgrade all DCs to Windows Server 2008. Raise the forest and domain function levels to Windows Server 2008. Install Windows Server 2003 on a member server and then run **dcpromo.exe** to install Active Directory on the member server, as a Replica Domain Controller for an existing Domain. Reinstall the application on the Windows Server 2003 DC.
 - D. Uninstall the application. Upgrade all DCs to Windows Server 2008, except for the DC that held the application. Move the Windows Server 2003 DC into its own Organizational Unit (OU). Raise the forest and domain function levels to Windows Server 2008. Reinstall the application.
7. You have been asked to provide a domain controller to a branch office. The office has 200 users, but no IT staff on site. One user in the branch office is competent enough that, if you needed him to do something with the Domain Controller, he would be able to assist with little help. Also, due to the layout of the office, there is no room in which to lock the server to provide physical security. What should you do to provide the branch location with a Domain Controller while not compromising security?
- A. Provide a DC to the branch and transfer the infrastructure master role to the DC. Add the competent user to the Domain Admins group.
 - B. Provide a DC to the branch and transfer the RID master role to the DC. Add the competent user to the Domain Admins group.
 - C. Provide a read-only domain controller (RODC) to the branch office and add the competent user to the Domain Admins group.
 - D. Provide a read-only domain controller (RODC) to the branch office and make the competent user a local administrator on the RODC.
8. You are planning the upgrade of your Windows Server 2003 Active Directory infrastructure to Windows Server 2008. What must you do before introducing the first Domain Controller running Windows Server 2008?
- A. Install Windows Server 2008 on a member server and join it to the domain. Add the computer object to the Domain Controller's Global Security group.
 - B. Install Windows Server 2008 on a member server and join it to the domain. Move the computer object to the Domain Controller's organization unit (OU).

- C. On the schema master run **adprep /forestprep**.
 - D. On the schema master run **regsvr32 schmmgmt.dll**.
9. You have been asked to assess the effect of an application in Active Directory. The application will add schema attributes, when installed. Your Active Directory forest is running at Windows Server 2008 forest function level. After testing the application you decide not to implement it. After you uninstall the application, you notice that the schema attributes which were added at installation are still present. You need to remove the effects of these attributes on Active Directory.
- A. Open Active Directory Schema. Browse through the attributes until you find the attributes you need to remove. Click the attribute, and on your keyboard press **Delete**.
 - B. Open Active Directory Schema. In the Properties of the attribute, select **Index this attribute**.
 - C. Open Active Directory Schema. In the Properties of the attribute deselect the attribute that is active.
 - D. Open Active Directory Schema. In the Properties of the attribute, in the **Syntax and Range** field, set both **Minimum** and **Maximum** values to **0**.
10. You are designing the Active Directory deployment of Windows Server 2008 Active Directory for a large organization with several branch offices. What are some factors to consider when deciding whether to use a read-only domain controller (RODC) as your only DC at a branch office location? Choose two answers to complete the solution.
- A. An RODC cannot hold the operations master tokens
 - B. An RODC should hold all operations master tokens
 - C. An RODC cannot hold the bridgehead server role
 - D. An RODC should hold the bridgehead server role

Self Test Quick Answer Key

- | | |
|------|----------|
| 1. C | 6. A |
| 2. D | 7. D |
| 3. A | 8. C |
| 4. C | 9. C |
| 5. A | 10. A, C |

Chapter 4

MCITP Exam 647

Designing an Enterprise-Level Group Policy Strategy

Exam objectives in this chapter:

- Understanding Group Policy Preferences
- Linking GPOs to Active Directory Objects
- Understanding Group Policy Hierarchy and Scope Filtering
- Controlling Device Installation

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

In Chapter 3, we looked at the different Active Directory Objects (ADOs) that make up the logical layout and the physical map of Active Directory. The logical layout comprises forests, trees, domains, and organizational units (OUs); the physical map is composed of domain controllers (DCs) and sites. In this chapter we are going to look at creating and linking Group Policy Objects or GPOs. It is important to understand the logical and physical layouts of Active Directory. It is equally important to understand how creating and linking GPOs might influence your logical or physical layout design.

Most companies today have two types of settings in place: managed and unmanaged, also known as locked-down and non-locked-down settings. Group policy is the best way to enforce either of these settings. In a managed environment, you as the administrator enforce policy settings. You do not allow the user to make changes to these settings. Examples of these settings include registry settings and the availability of certain Internet Explorer (IE) settings. In an unmanaged environment, you can still use Group Policy; but instead of creating policy settings, you can use Group Policy Preferences, which are settings that the user can either keep or change. These policy settings include profile settings, mapped drives, and so on.

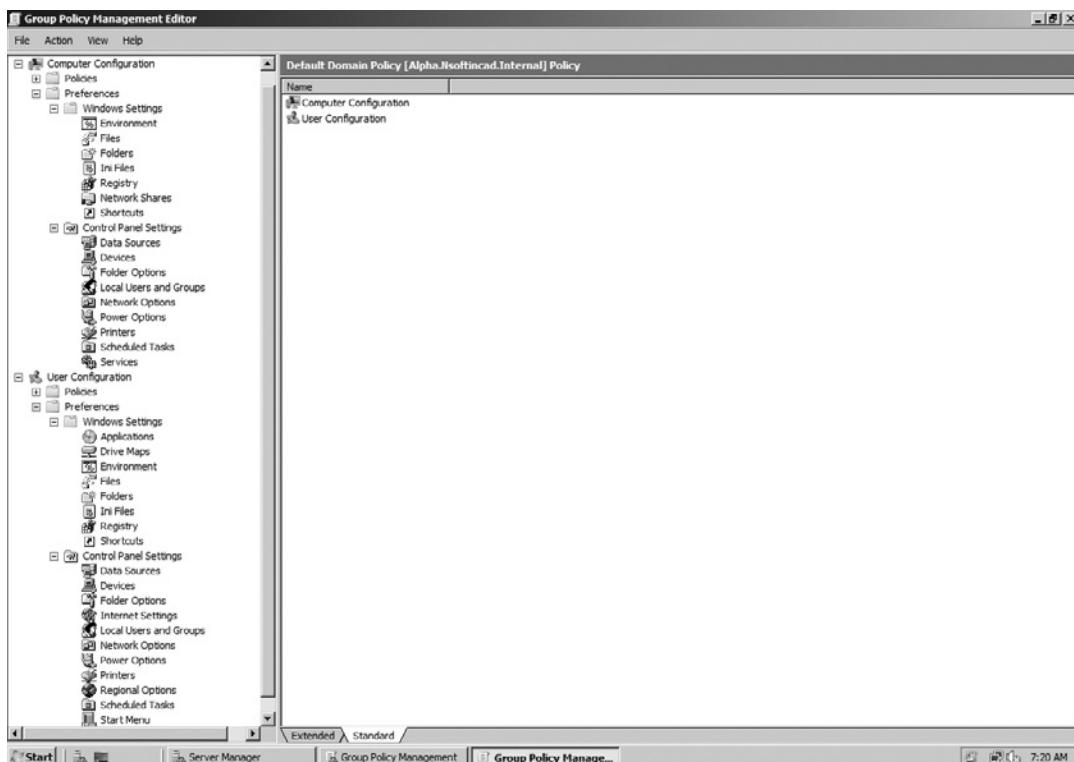
With the introduction of Windows Vista, and now Windows Server 2008, some changes have been made to Group Policy. Some of the changes that were made include:

- Group Policy Preferences
- ADMX\ADML Files

Understanding Group Policy Preferences

As we have just discussed, Group Policy Preferences are a way for the administrator to set policies that are not mandatory, but optional for the user or computer. These settings include the ability to add a shortcut to the desktop, to map a network drive, and to perform other common tasks that were previously only available through the use of logon scripts. See Figure 4.1 for an example of Group Policy Preferences.

Figure 4.1 Group Policy Preferences for Computer and User Configurations



Group Policy Preferences are located under Computer Configuration and User Configuration, and are then broken down further by Windows Settings and Control Panel Settings. Some of the common Computer Configuration tasks include using Windows Settings to configure INI files and environment variables, and using Control Panel Settings to configure Installing Printers and DSN (data source names) values. You can also specify shared folders, create scheduled tasks, and add registry keys. Some of the common User Configuration tasks include using Windows Settings to map network drives and manage desktop shortcuts and using Control Panel Settings to manage Regional Options and customize the Start menu. Remember that, even though these settings can be changed here in Group Policy, these policies will refresh on the client but will not stick if the user changes them. That is, the client can see and use the changes but is not married to them. The user can un-map the drive or change the environment variable, provided they have the appropriate rights to do so.

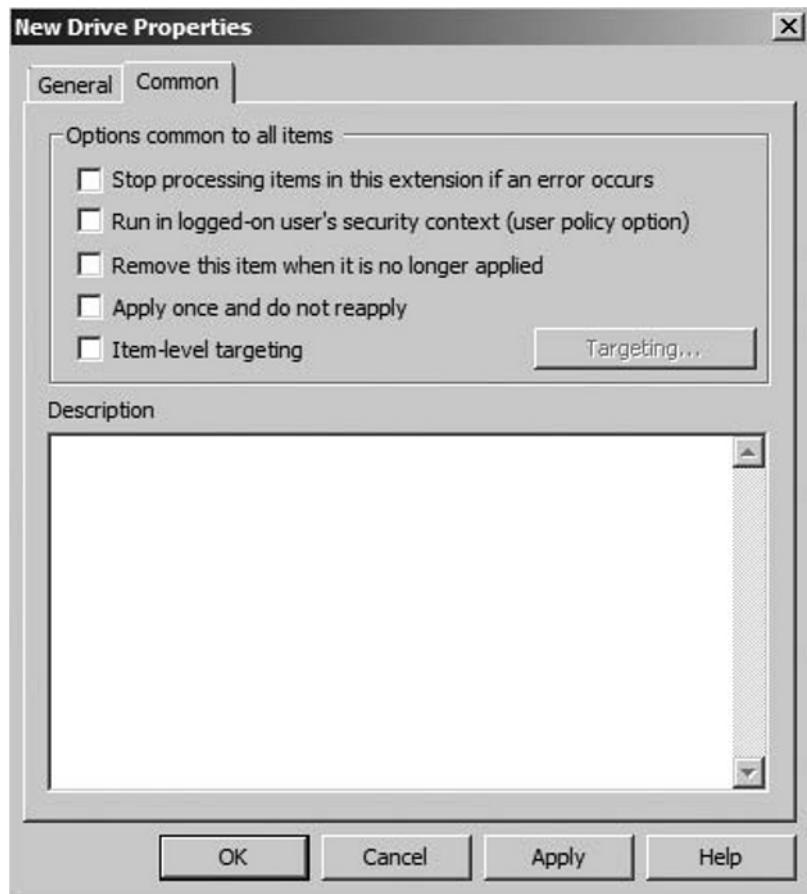
To map a network drive in Group Policy Preferences, follow the steps listed in Exercise 4.1.

EXERCISE 4.1

MAPPING A NETWORK DRIVE IN GROUP POLICY PREFERENCES

1. Log on as a user with rights to create Group Policies.
2. Open the **Group Policy Management Console** from Administrative Tools.
3. Create or modify a GPO.
4. Expand **User Configuration | Preferences**.
5. Click **Drive Maps**.
6. Right-click **Drive Maps** and then click **New | Mapped Drive**.
7. On the General tab you will have the option to do one of four tasks: Create, Replace, Update, or Delete. For this exercise, select **Create**.
8. In the **Location** field, type or browse to the network location of the shared folder, select the **Reconnect** check box, and then fill in the **Label as** field to give the drive map a descriptive name.
9. In the **Drive Letter** field, select either use first available, starting at or select the specific drive letter you wish to use.
10. In the **Connect as (optional)** field, type in a user name and password for the user account you wish to connect to the share as, if using a different account than the locally logged on user.
11. In the **Hide/Show this drive** field, select either **Hide this drive** or **Show this drive**.
12. In the **Common** tab, review **Options common to all items** and select from the list any option that you feel are required. (See Figure 4.2 for a list of these settings, which are optional.)
13. Click **OK**.

Figure 4.2 Common Options Available When Mapping a Drive with Group Policy Preferences



TEST DAY TIP

Group Policy Preferences is a new feature of Windows Server 2008 and, therefore, you will most likely see questions regarding this feature.

ADMX/ADMX Files

In previous versions of Group Policy, the Administrative Templates were a series of ADM files, or Administrative Template files. These files were pre-configured when you installed Active Directory. These settings when set would allow you to modify

specific settings on the client's registry in either **HKEY_LOCAL_MACHINE** (Computer Configuration settings) or **HKEY_CURRENT_USER** (User Configuration settings). The benefit of using them is that you did not need to know which registry key had to be modified. By using the pre-supplied templates, you set a setting, and the client would then incorporate your choice into the registry keys. However, the drawback to this arrangement was that the preconfigured settings were difficult to modify and create. For example, there is a setting under Computer Configuration called Hide These Drive Letters in Windows Explorer. This is a great setting to use if you want to limit access to the C:\ or other drives on the local machine. However, the options for this setting were limited. The choices were:

- Restrict All Drives
- Restrict C drive only
- Restrict D drive only
- Restrict A, B, C and D drives only
- Do not restrict drives

Also, if you wanted to restrict A and B or you wanted to restrict the M drive you would then have to modify the ADM template or write a custom script.

Today, ADM templates are written in XML (Extensible Mark-up Language). This means that they are more easily readable, and that more application vendors will be able to write more Administrative Template files, so that you can manage their applications using Group Policy. To get the added benefit of these ADMX files, you must launch the Group Policy Management Console (GPMC) from either a Windows Vista client or a Windows Server 2008 computer. Launching the console from a Windows XP computer will still show the files as ADM files instead of ADMX files.

The language-specific files for the different languages your Group Policy administrators might be working in, are called ADML files. As with ADMX files, you must use a Windows Vista or Server 2008 computer when launching the GPMC to see ADML files.

Another benefit of ADMX/ADML files and the way Windows Server 2008 uses them is that every GPO defined in a Windows 2000 or Server 2003 Active Directory environment had default ADM files associated with it and copied to it. Even if the GPO didn't touch the Administrative Templates. In Windows Server 2008, instead of the ADMX files being copied to each and every GPO created and, thus, replicating to all domain controllers, the ADMX and ADML files can be stored in a central repository. As a GPO requires access to the central repository, for example

to configure an Administrative Template setting, then it calls to the repository to use the appropriate file. This greatly reduces the amount of storage space necessary for maintaining your GPOs. By default, however, they are stored in the %systemroot%\PolicyDefinitions folder on each DC. If you choose to leave them there, then GPOs in Windows Server 2008 will behave the same way as in previous versions.

This central repository or store, however, is not created by default. To create and use the central store, follow the steps shown in Exercise 4.2. Note that it is recommended to do these steps on the PDC (primary domain controller) Emulator, and let the FRS (file replication service) copy the central store to all other DCs in your organization. For more information on the PDC Emulator, please see Chapter 3.

EXERCISE 4.2

CREATING THE CENTRAL STORE

1. Log on as a user with **Domain Admin** privileges or use the **runas** command.
2. Create a folder for the central store on the PDC Emulator called **%systemroot%\sysvol\domain\policies\PolicyDefinitions**.
3. Create a subfolder here for each language your Group Policy administrators will need, for example, **%systemroot%\sysvol\domain\policies\PolicyDefinitions\EN-US**.
4. Open a command prompt and then type the following and then press Enter: **copy %systemroot%\PolicyDefinitions* %logonserver%\sysvol%\userdnsdomain%\policies\PolicyDefinition**.
5. To copy the language specific ADM files (we will do United States English), type the following and then press Enter: **copy %systemroot%\PolicyDefinitions\EN-US* %logonserver%\sysvol%\userdnsdomain%\policies\PolicyDefinitions\EN-US**.

The variables in use here are the following:

- **%systemroot%** This is typically C:\Windows.
- **%logonserver%** This is the DC that authenticated your logon request.
- **%userdnsdomain%** This is your domain name. This is necessary because, if you are sitting locally at the machine (or using RDP) and using Windows Explorer to do the file copy, **Domain** is the next folder beneath

SYSVOL. However, if you are going over a network using the command prompt, your *domain name* is the next folder.

NOTE

You do not have to use a command prompt to copy the files. You may use Windows Explorer if you prefer. I am giving you these commands as a reference.

Once the store has been created and you have copied all of the ADMX and ADML files into the appropriate directory, your next step is to tell Group Policy to use these files from the central store. To do this simply open GPMC, create a new GPO, and then click **Edit**. Group Policy will look in this central location before looking in the default location. If it finds the ADMX files, it will use them and ignore the ADMX files in the %systemroot%\PolicyDefinitions folder. If you have created a central store and then modified an ADMX file that is still in the default location, GPMC will not notice this change as it is not merging the settings, but using the new centrally located files instead.

NOTE

If you had ADM files that were created or modified in your earlier versions of Windows, these files can still be used in Windows Server 2008 as long as there are no ADMX files that have superseded them, for example, System.admx or WUAU.admx. Your Custom.adm can still be accessed from its default location.

Understanding Group Policy Objects

Group Policy Objects (GPOs) are used to set configuration settings to sites, domains, or OUs. But they are *not* used to set configuration settings for groups. This is one of the biggest misnomers in Windows. Some of the configuration settings that can be set include registry-based settings, security settings, software deployment settings, logon scripts, folder redirection, and so on. These settings can either be set to be applied to the computer or the user. Managing the computer-based settings means that the settings take place upon startup (or Group Policy refresh)

regardless of who is physically logged onto the computer, if anyone. Applying the user-based settings means that depending on which user logs onto this computer a specific setting may or may not be set.

We have also discussed Group Policy Preferences. Like the other settings, these can be applied to either Computer Configuration or User Configuration. However, unlike the other settings, these settings can be changed once they have been applied.

The settings that you apply are created in containers known as Group Policy Objects. Like other Active Directory objects, these objects are defined by attributes, such as what settings have been enabled or disabled, and ACLs (Access Control Lists) so that AD knows to whom to apply the settings. To create the GPOs, you can use the Group Policy Management Console. Once a GPO has been created, it is stored in two places: The GPMC, and the SYSVOL folder on the domain controller. You can view and edit the GPOs using this file [which file?] in the SYSVOL folder – which can be found by , but you cannot create a GPO from here [where is here? please rewrite sentence so it's complete]. To view the Default Domain Controllers Policy using Windows Explorer, browse to C:\Windows\SYSVOL\sysvol\your domain name\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GPTTmpl.

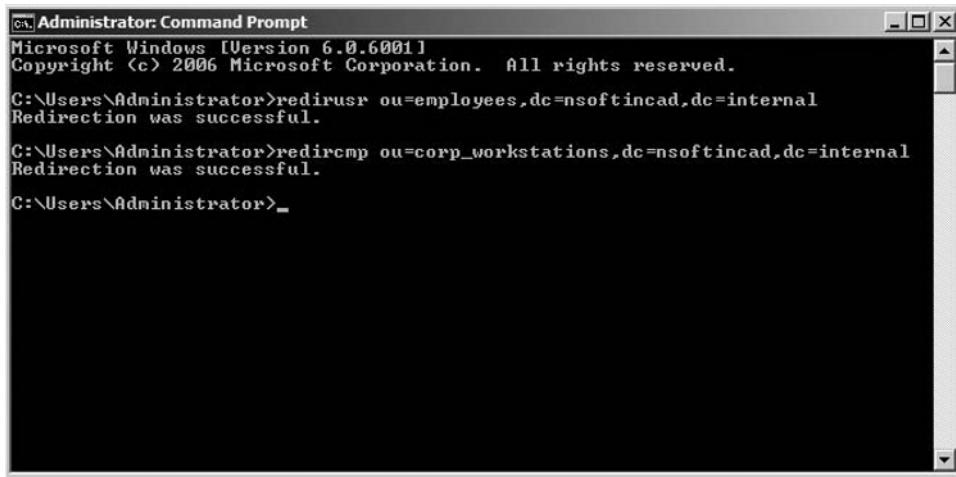
Now that you know where you can assign the policies, that is, to the computer upon reboot or refresh, or to the user upon logon or refresh, it is important to understand the process that must take place when planning and designing your Group Policy infrastructure. For example, we have already discussed that a GPO may be assigned to an Active Directory site, domain, or OU. But you must take GPO design into consideration when planning your OU structure as well. For example, if all of the users in your sales department must have a specific tracking application installed, it is easy to accomplish this if all of the users are in the same OU. Simply create a GPO, link it to the OU and deploy the software using the GPO. However, if your OU design has users from the sales department spread out over several different OUs, your GPO design will not be so easy.

And like other pieces of your design, always create a test environment before sending a GPO to all of your users or computers. You have already created a test environment for the design of Active Directory, and we discussed in Chapter 3 that this test environment should closely mirror the real environment, including OUs, users, and GPOs. It is in this environment where you should test the new GPOs.

One more thing to consider is that, even though you can link GPOs to OUs, you cannot link them to the default AD containers, such as the Users container or the Computers container. Therefore, it is possible that a new user or computer object will get created and not get the settings that would have been necessary

based on its role or job function. Therefore, Windows Server 2008 comes with commands that will allow you to redirect which container (or more importantly OU) will hold the newly created objects. The **redirusr.exe** and **redircmp.exe** commands can be used to redirect new user objects that are created through methods such as DSADD, and computer objects that are created when a workstation gets joined to the domain. See Figure 4.3 for examples of these commands.

Figure 4.3 Redirusr and Redircmp Commands

A screenshot of a Microsoft Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the following text:

```
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>redirusr ou=employees,dc=nsoftincad,dc=internal
Redirection was successful.

C:\Users\Administrator>redircmp ou=corp_workstations,dc=nsoftincad,dc=internal
Redirection was successful.

C:\Users\Administrator>_
```

The window has a standard Windows title bar and a scroll bar on the right side.

Other factors to consider when you are designing your Group Policy infrastructure are:

- Which DC will process GPOs
- Group Policy processing over slow links
- Group Policy processing over a remote connection
- Group Policy refresh interval
- Backing up and restoring GPOs

Deciding Which Domain Controller Will Process GPOs

As we discussed in Chapter 3, all domain controllers in an Active Directory forest are multimaster (except the read-only domain controller or RODC). This means that each DC can write to the Active Directory Domain Services (AD DS) database

and replicate that change to its replication partner. However, there are some changes that do not benefit from multi-master replication, for example, modifying the schema. So AD DS assigns certain roles to certain DCs. These roles are known as Operation Masters, or Flexible Single Master Operations (FSMO) roles. By default, Group Policy processing is given to the PDC Emulator in each domain. That means that whether you create a GPO and link it to the domain or the OU, the PDC Emulator is responsible for keeping track of changes to that GPO and replicating any changes to the other DCs in the domain. If you link a GPO to the Active Directory site, then the PDC Emulator in whichever domain you actually created the GPO in, will be responsible for that GPO, and will replicate the GPO and any changes to the other DCs in that site.

Of course, this default can be changed. The options for deciding which DC will be responsible for Group Policy processing can be changed either by using GPMC (Group Policy Management Console), as seen in Figure 4.4, or by setting the policy **User Configuration | Policies | Administrative Templates | System | Group Policy | Group Policy Domain Controller Selection**, as seen in Figure 4.5.

Figure 4.4 Which DC Will Process GPOs Using GPMC

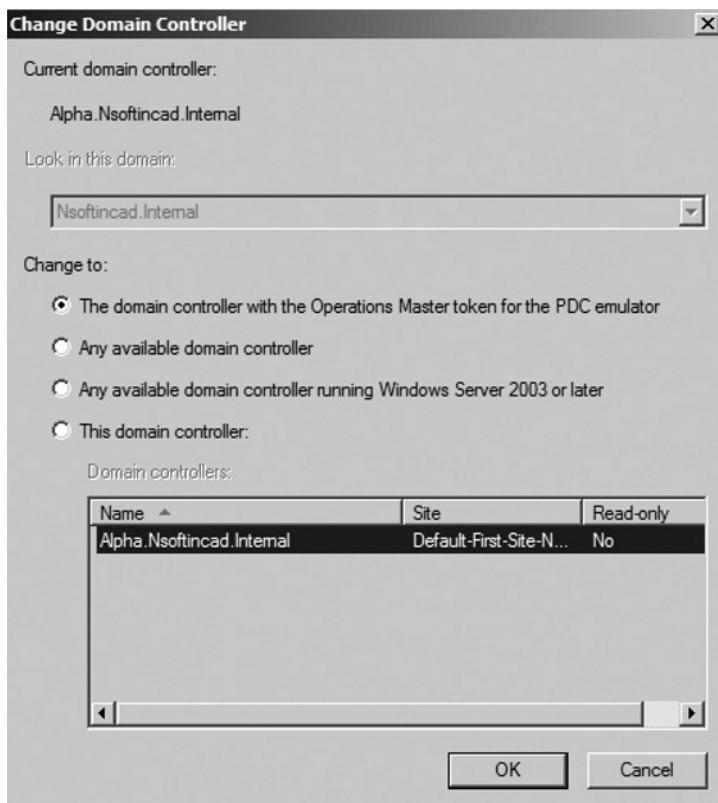
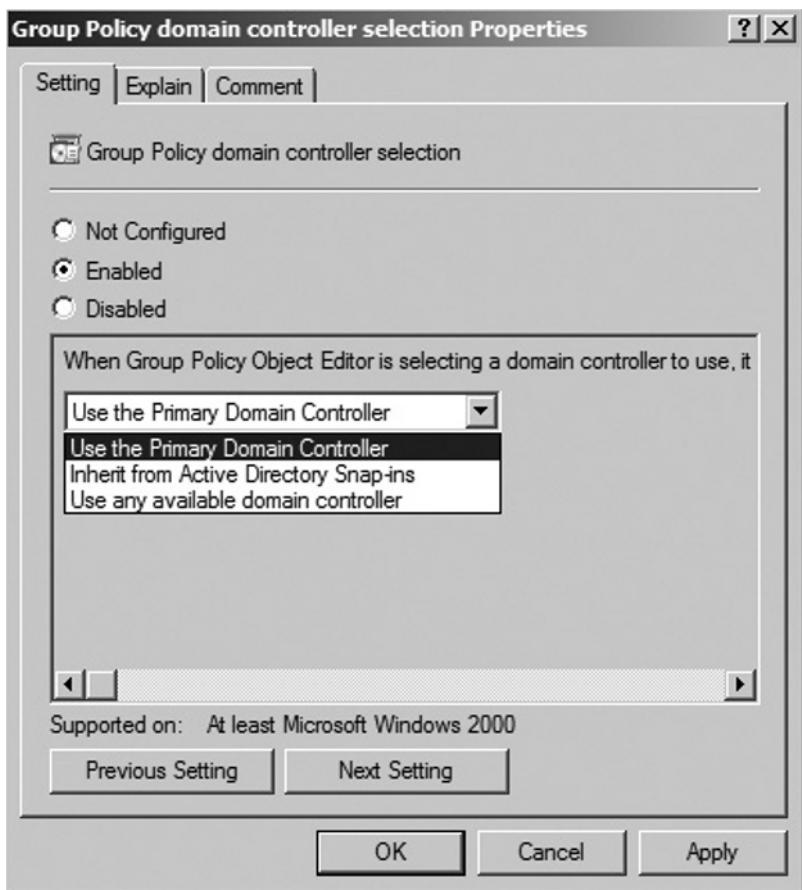


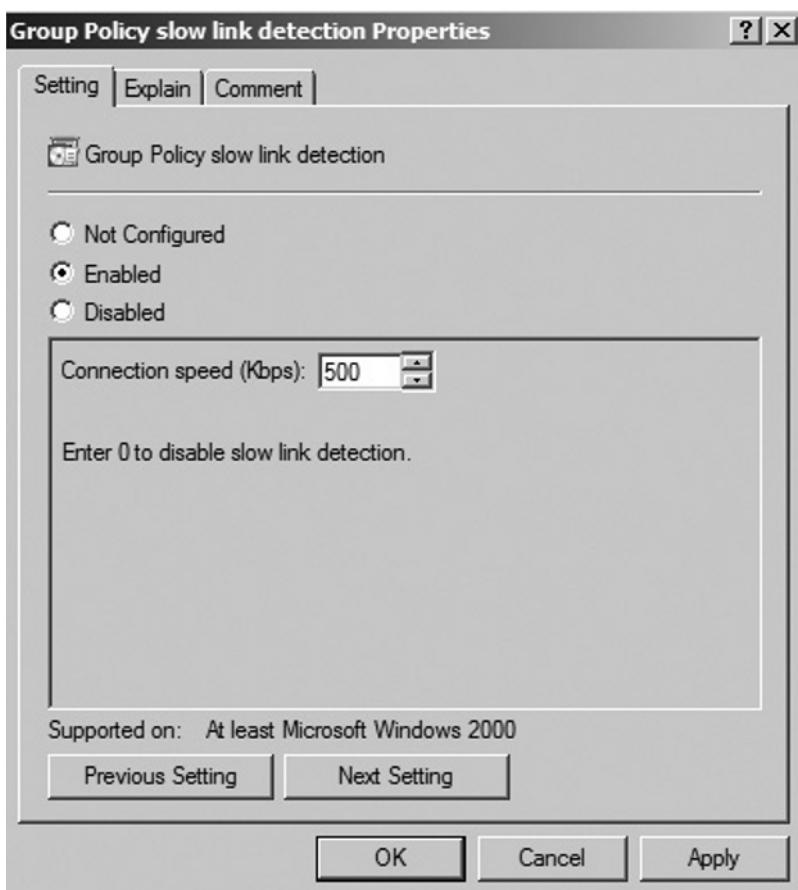
Figure 4.5 Which DC Will Process GPOs Using Group Policy

There are benefits and drawbacks to this default. By selecting the default, all Group Policy processing and, therefore, modifications are written to only one DC before being replicated to other DCs in your infrastructure. This is important for those administrators who do not want any replication conflicts. The drawback to using this default is that each domain has only one PDC Emulator. So if you are the GPO administrator, and you are in a location that has to cross a slow WAN link to get to the PDC Emulator, you may want to change this default to either **Any available domain controller running Windows Server 2003 or later** or to **This domain controller and then select the closest domain controller to your location**.

Group Policy Processing over Slow Links

There are certain policies that will not be applied when you are refreshing GPOs over a slow WAN link, for example software deployment. However, there are also certain policies, such as the Security policies that will apply regardless of the speed of the link during the refresh. Group Policy will detect the network speed each time a refresh happens, whether it is during startup, logon, or the automatic refresh interval (which is 90 minutes per workstation by default). Upon Group Policy refresh, Group Policy will detect link speed and, if the speed is deemed to be slower than 500 Kbps (Kilobits per second), it will consider it to be a slow link. The slow WAN link is configurable by setting the policy **Computer Configuration | Policies | Administrative Templates | Group Policy | Slow link detection**. Note that this policy can also be set under User Configuration to detect the link speed for user-side policies. See Figure 4.6.

Figure 4.6 Slow Link Detection Policy



Group Policy processing happens over three phases: preprocessing, processing, and post-processing phase. During the preprocessing phase, Group Policy gathers information, such as the location of the domain controller. During the processing phase, Group Policy processes all of the policies based on the information gathered during the preprocessing phase. For example, if during the preprocessing phase, Group Policy determined a slow WAN link between the client and the DC, the processing phase would take that into consideration when processing the policies. During the post-processing phase, your logs get written to the Event Viewer indicating whether a successful or failed attempt to process the GPOs occurred.

The way that GPO detects the link speed has been improved since Windows Server 2003. In Windows Server 2003, Internet Control Message Protocol (ICMP, also known as ping) packets were sent from the client to the domain controller, and the return trip was timed. In Windows Server 2008, the NLA (Network Location Awareness) service is used to test the current speed of Transmission Control Protocol (TCP) traffic over the link. This happens during the preprocessing phase. As we have discussed, certain policies will be excluded from processing if the NLA service deems the link slower than 500 Kbps. Use Table 4.1 to determine if the policy will be applied.

Table 4.1 GPO Settings Applied During Slow Link Detection

| Setting | Default (Will Be Processed?) | Can be changed? |
|-------------------------------|------------------------------|-----------------|
| Security Settings | ON | NO |
| IPSec Settings | ON | YES |
| EFS Settings | ON | YES |
| Software restriction Policies | ON | YES |
| Wireless Settings | ON | YES |
| Administrative Templates | ON | NO |
| Scripts | OFF | YES |
| Folder Redirection | OFF | YES |
| QoS Policies | ON | YES |
| Disk Quota Policies | OFF | YES |
| IE Zone Mapping Policy | ON | YES |

Continued

Table 4.1 Continued. GPO Settings Applied During Slow Link Detection

| Setting | Default (Will Be Processed?) | Can be changed? |
|--------------------------|------------------------------|-----------------|
| IE Maintenance | ON | YES |
| Group Policy Preferences | ON | YES |
| Windows Search | ON | YES |
| Printer Deployment | OFF | YES |
| 802.3 Policies | ON | YES |
| Offline Files Policy | ON | YES |

Group Policy Processing over Remote Access Connections

Don't get confused between slow links and remote access. Just because you are connected to the LAN does not mean you have a reliable high-speed network. And just because you are traveling across a remote access connection does not mean that the connection is slow. Therefore even over a remote access connection, Group Policy has to determine the speed of the link between the client and the DC.

Over a remote access connection, the user starts his computer before connecting to the remote access server. Therefore upon startup, there is no policy processing.

However, if the user, prior to logging on, selects the option to log on over the remote access connection, then upon logon, both the Computer policies and the User policies will be applied, provided that the computer is a member of the domain. However, any Software Installation policies or Start Up scripts will not run over the remote access connection because they would be processed before the User Logon screen. If the user logs onto the workstation without selecting the **Logon over a Remote Access connection** check box, then the user gets logged on with cached credentials. If they then use their virtual private network (VPN) software to connect to the network, then the policies will be applied during the refresh interval only.

Group Policy Background Refresh Interval

By default, group policies are applied at computer startup and at user logon. After that, however, Group Policy will refresh at predetermined time intervals. Depending on the type of computer, that is a workstation, a member server, or a domain controller, the

background refresh interval will be different. To set the time interval of the background refresh for workstations, modify **Computer Configuration | Policies | Administrative Policies | System | Group Policy | Group Policy refresh interval for computers**. As explained on the Explain tab of this setting, this range can be from 0 to 64800 minutes (45 days). If you set this to 0, then the background refresh will occur every 7 seconds. However, this policy will most likely interfere with user work productivity. Also, you can set this policy setting for User Configuration as well for the user-side policy refresh.

The default setting, even if this policy setting is set to Not Configured, is 90 minutes. This has a 30-minute offset, which means that the background refresh will occur roughly every 90 minutes, give-or-take 30 minutes. This way, if all of your users start their computers at 9 A.M., then the refresh will not happen at 11:30 A.M. and then again at 1:00 P.M. for each and every computer in your organization. It will be a random offset of up to 90 minutes for each computer. There is also a setting that will turn-off Background refresh, in case you want to ensure that policies only get applied during startup and logon. If you set this setting, the computer will update the user-side policies at logoff. This setting can be set at **Computer Configuration | Policies | Administrative Policies | System | Group Policy | Turn off background refresh of Group Policy**. This is only a Computer Configuration setting, and will require a restart to actually be set on the client.

Group Policies refresh on domain controllers in the same way as for workstations. That is, GPOs are applied at startup, logon and at the background refresh interval. The background refresh interval for DCs, however, is every 5 minutes. Of course this is configurable as well.

If you set a new policy, and do not wish to wait the 90 minutes for the setting to apply, you can instruct the user to run a command to refresh group policies. This command will update all of the policies, not a specific setting. You can, however, specify to refresh only User Configuration or only Computer Configuration. The command to force a refresh of Group Policy is **gpupdate /force**. For more command options available, type **gpupdate /?**. Other options include specifying Computer Configuration or User Configuration only, whether you want to forcibly reboot or logoff, and if you want to set a wait value to specify how long Group Policy processing should wait before timing out.

Backing Up and Restoring GPOs

Back in the days of Windows 2000 Active Directory, when group policies were still new, the only way to back up your policies was to do a System State backup, which

would back up your entire Active Directory database, as well as other pieces of the domain controller. With Windows Server 2003, Active Directory came up with a command to roll back to the default states the Default Domain Policy and the Default Domain Controllers Policy. To do this, use the command **dcpofix.exe**. However, it is important to note that these policies will be set back to their defaults. Any changes that were made to these policies will be lost. Also, the **dcpofix.exe** command will only restore the Default Domain Policy and the Default Domain Controllers Policy, and not other policies that the GPO administrator may have created. For a list of available commands, type **dcpofix.exe /?**. Some of the available commands include specifying whether you are restoring the Default Domain Policy or the Default Domain Controller Policy, and specifying whether to ignore the specific Windows Server 2008 schema changes.

It is a good idea to back up all of the GPOs in case you need to revert back to an earlier version in the case of a catastrophic event. To back up the rest of your GPOs (including the Default Domain Policy and the Default Domain Controllers Policy), use the Group Policy Management Console (GPMC). You can use GPMC to either backup a specific GPO, or to back up all of the GPOs. To back up all GPOs, follow the steps shown in Exercise 4.3. Note that in order to back up the GPOs you must have read access to the Group Policy Object, and write access to the folder that they are being backed up into.

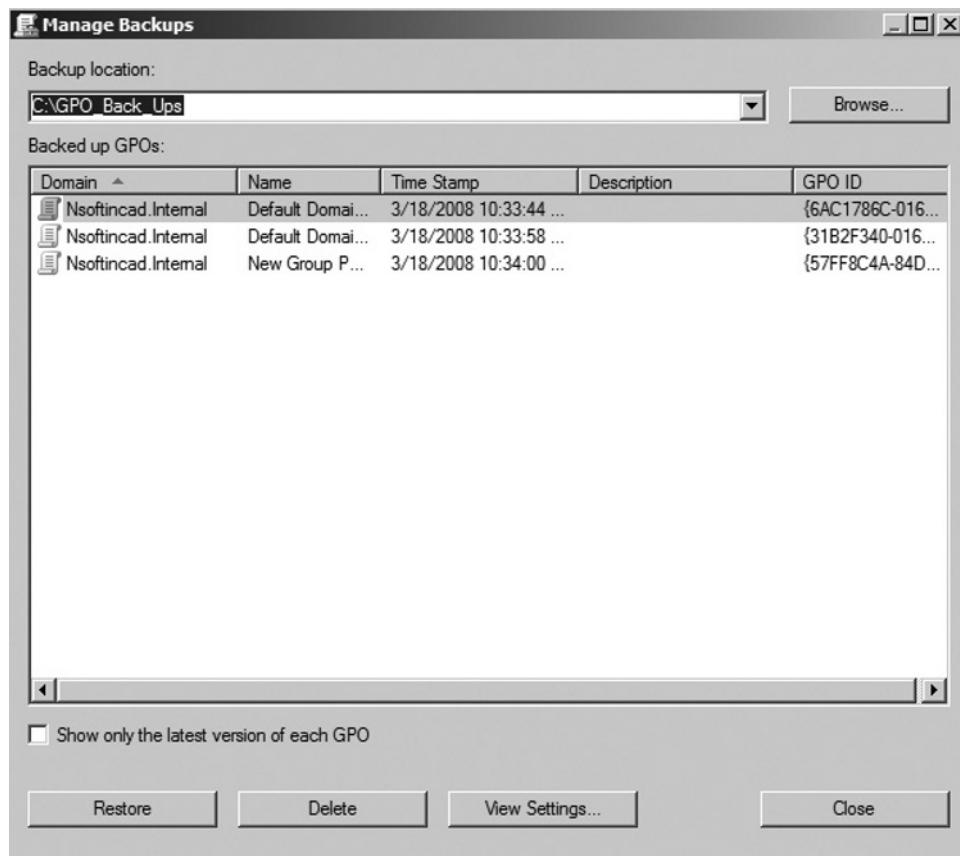
EXERCISE 4.3

BACKING UP GROUP POLICY OBJECTS

1. Launch Group Policy Management Console.
2. Expand Forest: *your forest name*.
3. Expand **Domains** | *your domain name*.
4. Right-click **Group Policy Objects**, and then select **Back Up All**.
5. In the **Back Up Group Policy Object** dialog box, in the **Location** field, type or browse to the location in which you would like the backup placed.
6. In the **Description** field, type an optional description.
7. Click **Back Up**.
8. On the **Backup progress** page, ensure the **Status** displays as **Succeeded** for each GPO, and then click **OK**.

Once these are backed up, you would then use the GPMC to restore the GPOs to the previous state. Even though the backups are located in a folder in Windows Explorer, you always use GPMC to manipulate or view the contents of the backed up GPO. To manage the backups in the GPMC, right-click **Group Policy Objects**, and then select **Manage** backups. Notice in Figure 4.7 the options available to restore or delete a GPO backup, or to view the settings of the backup.

Figure 4.7 GPMC Manage Back Ups



To restore a GPO to a previous version, provided that the GPO has not been deleted from GPMC, follow the steps shown in Exercise 4.4. Note that you must have write access to the GPO, and read access to the folder holding the backups.

EXERCISE 4.4

RESTORING A GPO TO A PREVIOUS VERSION

1. Launch **Group Policy Management Console**.
2. Expand Forest: *your forest name*.
3. Expand **Domains** | *your domain name*.
4. Right-click **Group Policy Objects**, click the GPO you wish to restore back to an earlier version, and select **Restore from backup**.
5. On the **Welcome** page in the Restore Group Policy Object Wizard, click **Next**.
6. On the **Backup Location** page, in the **Backup** folder field, type or browse to the backup folder location, and then click **Next**.
7. On the **Source GPO** page in the backed-up GPOs window, verify that the source GPO is selected, and then click **Next**. (You may view the settings of the backup prior to restoring by clicking **View Settings**.)
8. On the **Completing** page, click **Finish**.
9. On the **Restore progress** page, ensure the **Status** displays as **Succeeded**, and then click **OK**.

If the GPO that needs to be restored has been deleted from GPMC, use the steps above to manage backups, and then select the **Restore** button.

User Policies

As we have learned already, Group Policy Objects are separated into two sections: the Computer Policy and the User Policy. User policy settings get applied to the user accounts after logon. Determining how many GPOs are required for your users takes planning and depends on a number of factors including your domain and OU design, your network speed between your locations, what you are trying to accomplish with Group Policy, and so on. And some domains in your organization will require less GPOs than other domains. But the number of GPOs applied to a user, and the number of settings inside those GPOs will greatly affect logon times. Examples of settings that you might apply to the user accounts include Software Installation, Security Settings, Folder Redirection Settings, Logon and Logoff Scripts and Administrative Templates.

Software Installation

Installing software by using Group Policy enables on-demand software installation and self-healing applications. When you create a Software Installation package under User Configuration, it is important to note that the application will not get installed automatically. The user will need to “call” the application installation. That can happen in one of three ways:

- Adding or removing the Programs Control Panel applet
- Invoking file invocation
- Launching the application’s Start menu shortcut

The method available to the user will depend on how you have made it available; that is, did you *assign* the package to the user, or did you *publish* the package.

To assign a Software Installation Package, follow the steps shown in Exercise 4.5.

EXERCISE 4.5

ASSIGNING A SOFTWARE INSTALLATION PACKAGE

1. Create a new GPO or edit an existing one.
2. Expand **User Configuration | Policies | Software Settings**.
3. Right-click **Software installation** and then click **New | Package**.
4. In the Open dialog box, type in the network location of the installation file (MSI) using a universal naming convention (UNC) path.
5. In the Deploy Software dialog box, select **Assigned**, and then click **OK**.
6. Right-click the new package and then click **Properties** if you want to set any additional deployment options, such as whether this package will upgrade an existing package or assigning it to a category in Control Panel.

NOTE

If you wish to deploy the package as an upgrade, or need to specify an MST (Transform) file to the package, or would like to set any of the other options available from the properties of the package, you should select **Advanced** in Step 5 instead of **Assigned**. This will allow you to assign the package and set the properties all at once.

**TEST DAY TIP**

It is possible to set certain defaults in this New Package Wizard. Some of the more common defaults to set are the Distribution Folder path, and Categories in Control Panel.

Security Settings

Security Settings are typically set at the Computer Configuration. Because of this, there are only two containers inside the Security Settings container within the User Configuration section of Group Policy. These containers have the settings that apply to Public Key Policies and Software restriction Policies.

Public Key Policies are used to Import certificates from either Enterprise Trust or Trusted People. Enterprise Trust provides a mechanism for trusting self-signed root certificates from other organizations, and Trusted People are certificates issued to those that are specifically Trusted, such as your Outlook contacts.

Software restriction Policies allow you to identify which software is allowed to run on your organization's workstations. These policies can be defined by Security Levels or Additional Rules. The Security Levels are further broken down into Disallowed, or this program is not allowed to run; Basic User, this program can run using the credentials of a non-admin account; Unrestricted, the user's credentials determine whether or not the program can run. Additional Rules that you can create are:

- **Certificate Rule** Identifies software by its signing certificate, then the rule allows the software to run or disallows it from running depending on the security level.

- **Hash Rule** Uniquely identifies a program using a series of bytes. When you create a Hash Rule, Software Restriction Policy calculates an algorithm for the program. When a user attempts to launch the program, the hash is compared to that of the Software Restriction Policy.
- **Network Zone Rule** Identifies software from a zone, which is specified in Internet Explorer.
- **Path Rule** Identifies software program by its path, for example, C:\Windows\System32\Calc. It is common, however, to set a Path Rule to Unrestricted by using a path like %userprofile%, %appdata%, and so on.

Folder Redirection Settings

When folder redirection first came out in Windows 2000 Active Directory, the most commonly used setting was that of redirecting the My Documents folder to a network share. The benefit of this was that your users would still save their documents into the My Documents folder; however, they were also being stored over the network, making backups much easier. The other settings in Windows 2000 were redirecting the Desktop, My Music (which was a subset of My Documents), and the AppData directory. Today, the following folders can be redirected using Group Policy folder redirection:

- AppData
- Desktop
- Start Menu
- Documents
- Pictures
- Music
- Videos
- Favorites
- Contacts
- Downloads
- Links
- Searches
- Saved Games

You will notice that most of these are typically in the Documents folder. However, they can be redirected to different locations, based on the type of content. For example, all Music folders redirected to a multimedia server, while all folders under the Documents folder are redirected to a file server.

Other benefits of folder redirection include having the user's My Documents folder "follow" the user to whichever computer he logs onto, and allowing the user's data to be redirected to a partition other than the system partition, in the case that the user's operating system needs to be rebuilt.

TEST DAY TIP

 You will likely see questions regarding folder redirection. However, it is unlikely that questions will delve into which folders can be redirected and which ones cannot.

To redirect everyone's Documents folder to the same network location, create a shared folder on a file server, grant the users group Full Control to the Share and NTFS permissions, and then follow the steps shown in Exercise 4.6.

EXERCISE 4.6

REDIRECTING DOCUMENTS FOLDERS TO THE SAME NETWORK LOCATION

1. Create a new GPO or edit an existing one.
2. Expand **User Configuration | Policies | Windows Settings | Folder Redirection**, and then click **Documents**.
3. Right-click **Documents**, and then click **Properties**.
4. In the **Documents Properties** dialog box, on the Target tab, in the Setting field, select **Basic-Redirect everyone's folder to the same location**.
5. In the Target folder location field, select **Create a folder for each user under the root path**.
6. In the Root Path field, type the UNC path to the network location created earlier.

7. On the Settings tab, ensure that **Grant the user exclusive rights to Documents** and **Move the contents of Documents to the new location** are selected. Optionally, select the option **Also apply redirection policy to** for the appropriate operating system: Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003.
 8. In the Policy Removal section, select whether to leave these files here or redirect them back to their default location when the policy is removed.
 9. Click **OK**.
-



NOTE

Setting **Grant the user exclusive rights to Documents** will ensure that, even though you gave the users group full control to the share, only the specified user will have access to this folder.

Logon and Logoff Scripts

There are two events that will trigger the Group Policy User Configuration scripts to run: logon and logoff. These scripts do not run during the background refresh every 90 minutes. They are exclusive to log on and log off. If a logged-on user shuts down his computer from the Start menu, the logoff scripts will run, and then the computer will shut down. Keep in mind that a Logon script or a logoff script will run under the credentials of the logged on user, so make sure the user has the appropriate access to the pieces of the operating system required by the script.

Logon scripts can be written in any language the WSH (Windows Scripting Host) can understand. These languages include Visual Basic (VB), VBScript, Jscript, and BAT files. It is important to note that Group Policy does not write the script. It can call a script that has already been written. To assign a logon script through Group Policy, follow the steps shown in Exercise 4.7, while logged on as a user with write permission to the GPO.

EXERCISE 4.7

ASSIGNING A LOGON SCRIPT THROUGH GROUP POLICY

1. Copy the predefined script to the **netlogon** share on the PDC Emulator.
2. Create a new GPO or edit an existing one.
3. Expand **User Configuration | Policies | Windows Settings**, and then click **Scripts**.
4. In the Details pane, double-click **Logon**.
5. In the **Logon Properties** dialog box, click **Add**.
6. In the **Add a Script** dialog box, in the **Script Name** field, type or browse to the location of the script.
7. In the **Script Parameters** field, add any parameters such as **/qb** to run quietly in the background.
8. Repeat Steps 5 through 7 until all scripts have been added and then click **OK**.

NOTE

These scripts will run from the top script down to the last script in that order. You can use the **Move up** and **Move down** buttons to reorder the script processing order.

TEST DAY TIP

The process for linking logoff scripts is the same, except that you double-click **Logoff** in Step 4.

Administrative Templates

As discussed earlier in the chapter, all of the Administrative Templates alter some key in the registry database under the hive **HKEY_CURRENT_USER**. The benefit of using the Administrative Templates to alter these keys is that you do not need to know the key to modify it. We have also discussed that the Administrative Templates are written in XML in a file called an ADMX file, and are now language-specific for your GPO administrators in files called ADML files.

Prior versions of Active Directory and Group Policy used a file that was written in its own type of mark-up language. These files were ADM files, and can still be used today. If an application vendor has supplied you with an ADM file to assist in managing their application, you can still use the ADM file while also using the ADMX files for other areas of the operation system. However, if an ADMX file has been created that supersedes an ADM file, for example, System.admx, then the ADMX will be used. So any changes that have been made to your system.adm file will not be recognized by Group Policy. Therefore, Microsoft has created an ADMX Migrator tool that is an MSC snap-in and that will simplify the process of converting your ADM templates into ADMX file format, and will even give you a GUI (graphical user interface) for creating ADMX files. The ADMX Migrator tool can be downloaded from Microsoft's download center.

New to the Administrative Templates in Windows Server 2008 is the ability to add comments to each setting. Simply expand the group policy until you find the setting you wish to comment, go to the setting's **Properties** dialog box, click **Comments**, and then add a comment. Another new field to these Administrative Templates is the **All Settings** field. Have you ever looked for a Group Policy setting and was not sure where it was located, for example, under Control Panel or Windows Components? Since there is no search feature inside the Group Policy Management Editor, finding these settings was challenging, at best. Now you can click the **All Settings** container, and all of the settings, regardless of which Administrative Template they are located in, are listed with the path to where they are found. See Figure 4.8 for details. You can configure the setting from the listing, or you can browse to the setting's location within Administrative Templates and configure it from there. The following subfolders exist under Administrative Templates, many of which have subfolders of their own:

- Control Panel
- Desktop
- Network

- Shared Folders
- Start Menu and Taskbar
- System
- Windows Components
- All Settings

Figure 4.8 Administrative Templates All Settings

The screenshot shows the 'Group Policy Management Editor' window. The left pane displays a tree view of policy settings under 'Sales Application [Alpha.Nsoftincad]'. The 'Administrative Templates' node is expanded, showing sub-nodes for Control Panel, Network, Printers, System, Windows Components, and All Settings. The 'All Settings' node is also expanded, showing numerous specific policy items such as '.Net Framework Configuration', 'Ability to change properties of an all user remo...', and 'Ability to delete all user remote access connect...'. The right pane is a table titled 'Setting' with columns for 'Setting', 'State', 'Comment', and 'Path'. The table lists 1332 setting(s). At the bottom, there are tabs for 'Extended' and 'Standard', and a status bar showing 'Group Policy Management' and the time '4:51 AM'.

| Setting | State | Comment | Path |
|--|----------------|---------|-------------------------|
| .Net Framework Configuration | Not configured | No | \Windows Components\W |
| Ability to change properties of an all user remo... | Not configured | No | \Network\Network Conne |
| Ability to delete all user remote access connect... | Not configured | No | \Network\Network Conne |
| Ability to Enable/Disable a LAN connection | Not configured | No | \Network\Network Conne |
| Ability to rename all user remote access conn... | Not configured | No | \Network\Network Conne |
| Ability to rename LAN connections | Not configured | No | \Network\Network Conne |
| Ability to rename LAN connections or remote a... | Not configured | No | \Network\Network Conne |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Access data sources across domains | Not configured | No | \Windows Components\Ur |
| Action on server disconnect | Not configured | No | \Network\Offline Files |
| Active Directory Domains and Trusts | Not configured | No | \Windows Components\W |
| Active Directory Sites and Services | Not configured | No | \Windows Components\W |
| Active Directory Users and Computers | Not configured | No | \Windows Components\W |
| ActiveX Control | Not configured | No | \Windows Components\W |
| Add "Run in Separate Memory Space" check bo... | Not configured | No | \Start Menu and Taskbar |
| Add a specific list of search providers to the us... | Not configured | No | \Windows Components\Ur |
| Add Logoff to the Start Menu | Not configured | No | \Start Menu and Taskbar |

Computer Policies

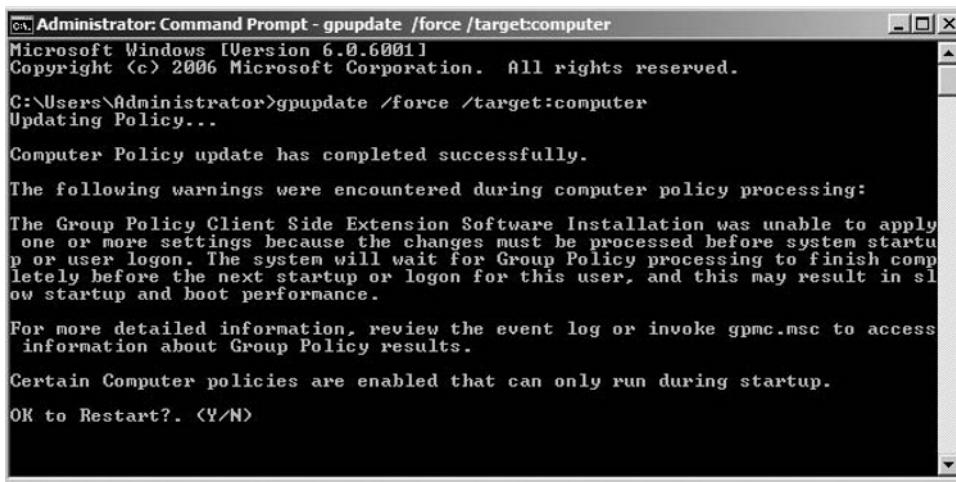
The Computer-side policy settings get applied during startup. Windows does not differentiate between a clean start and a reboot. Either way, computer policies apply as the computer boots up. Like user policies, the greater number of policies created, and the greater number of set settings in these policies, the longer each startup will take. So keeping these policies to a minimum, and grouping together “like”

settings into a single policy or only a few policies, will reduce the amount of time Windows takes to startup. Examples of common settings set at the computer-side are software installation, security (such as Restricted Groups and Windows Firewall with Advanced Security), policy-based QoS, startup and shutdown scripts, and Administrative Templates.

Software Installation

Just like its user-side counterpart, software installation through Group Policy offers a way to install applications (either OU-wide, domain-wide, or site-wide) without touching the computers. However, unlike the user-side counterpart, these applications get installed without the user calling them. Instead of on-demand application installation, the application gets installed at reboot. Software installation settings do not apply during the background refresh interval. And, if a user types **gpupdate** from a command prompt window after the GPO administrator assigns a new software installation package to a GPO, they will then be prompted to restart the computer to get the application. See Figure 4.9.

Figure 4.9 GPUpdate after New Software Installation Package Requests a Restart



```
Administrator: Command Prompt - gpupdate /force /target:computer
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force /target:computer
Updating Policy...

Computer Policy update has completed successfully.

The following warnings were encountered during computer policy processing:

The Group Policy Client Side Extension Software Installation was unable to apply
one or more settings because the changes must be processed before system startu
p or user logon. The system will wait for Group Policy processing to finish comp
letely before the next startup or logon for this user, and this may result in sl
ow startup and boot performance.

For more detailed information, review the event log or invoke gpmc.msc to access
information about Group Policy results.

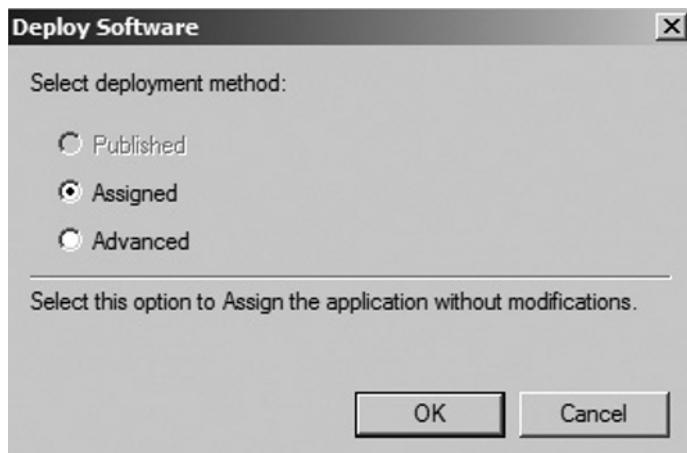
Certain Computer policies are enabled that can only run during startup.

OK to Restart?. <Y/N>
```

Also unlike the user-side counterpart, there is only one option you can use when creating the package: **Assign**. Remember, in the user software installation package, you can either **Assign** or **Publish**. In the computer-side, you can

only assign. Assigning a package means that it will be installed at the next startup. Therefore, a transform file or some other way of answering the installation questions must be configured. See Figure 4.10 for the New Package Wizard in the Computer Configuration section of the Group Policy Management Editor. (Note that in Figure 4.10 the Published option is not available.)

Figure 4.10 Computer Configuration New Package Wizard



Restricted Groups

By using the Restricted Groups feature in Group Policy, you are ensuring that the security groups in use in your organization will have specific members only, and can become members of only specific groups. For example, if a user logs on to an administrator account and adds himself to the Administrators group on his workstation, Restricted Groups will ensure that he is removed the next time Group Policy refreshes. Another common use for Restricted Groups is the Enterprise Admins and Schema Admins Security groups. Since these groups are special groups which have enterprise-wide affect, it is common to use Group Policy Restricted Groups to ensure that only certain users have been added to these groups. And since Group Policy refresh happens every five minutes on domain controllers, your policy will have an almost immediate effect.

To use Group Policy to ensure the administrator is only a member of the Enterprise Admins group, log on as a Domain Admin on the forest root domain or use the **runas** command, and follow the steps shown in Exercise 4.8.

EXERCISE 4.8

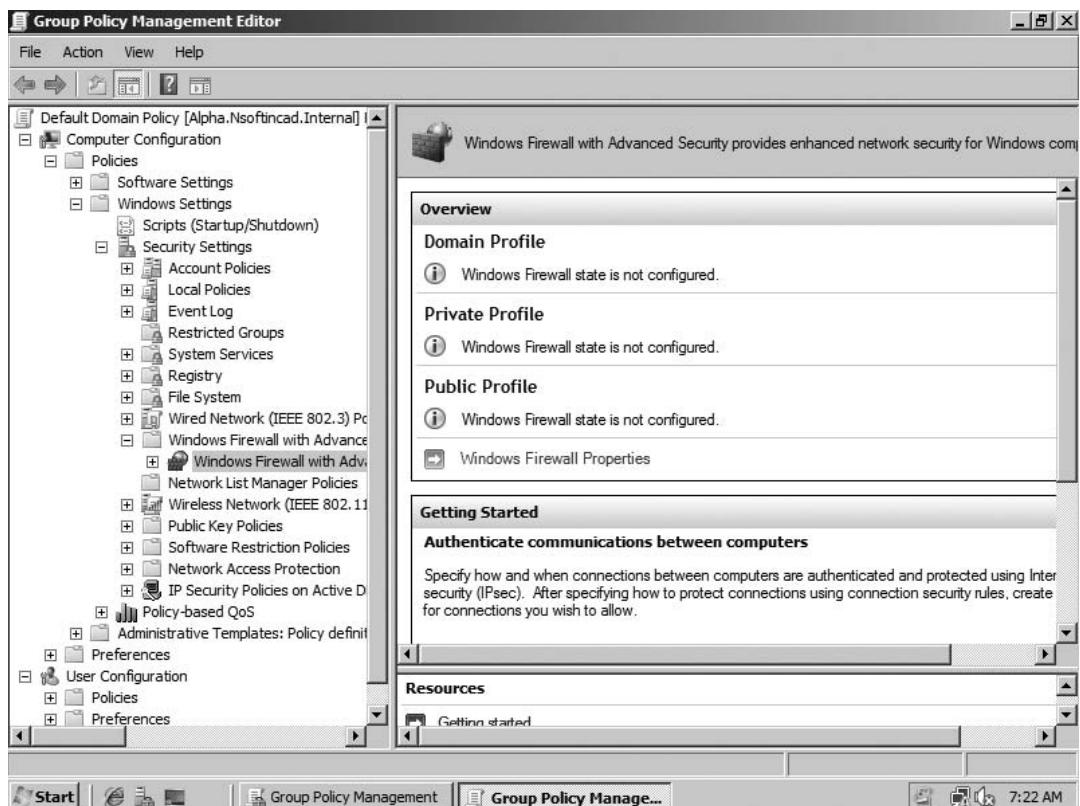
SETTING THE ADMINISTRATOR AS THE ONLY MEMBER OF THE ENTERPRISE ADMINS GROUP

1. Create a new GPO or edit an existing one.
2. Expand to **Computer Configuration | Policies | Windows Settings | Security Settings | Restricted Groups**.
3. Right-click **Restricted Groups**, and then click **Add Group**.
4. In the **Add Group** dialog box, in the **Group** field, type or browse to *domain\Enterprise Admins*, and then click **OK**.
5. In the *domain\Enterprise Admins Properties* dialog box, in the **Members of this group** field, click **Add**.
6. In the **Add Member** dialog box, in the **Members of this group** field, type or browse to *domain\Administrator*, and then click **OK**.
7. To make the Enterprise Admins group a member of another group, in the **This group or as a member of** field, click **Add**.
8. In the **Group Membership** dialog box, in the **Group** field, type or browse to the group that you wish to add the Enterprise Admins as a member, and then click **OK**.
9. In the *domain\Enterprise Admins Properties* dialog box, click **OK**.

Windows Firewall with Advanced Security

The Windows Firewall with Advanced Security is a new MMC snap-in that enables administrators a lot more functionality than the old Windows XP SP2 firewall. This firewall has been integrated with IP Security Protocol (IPSec) to give a single interface from which you can specify what traffic will be allowed to be sent or received when connected to the domain or, when sitting in a public location, what will be encrypted, and so on. By using Group Policy, you can configure multiple computers at one time without the need to export settings from one computer and import into another. One of the benefits of using Group Policy to configure this advanced firewall is the interface within Group Policy. See Figure 4.11 for the interface in Group Policy Management Editor. For more information on using the Windows Firewall with Advanced Security, see Chapter 2.

Figure 4.11 Windows Firewall with Advanced Security Group Policy Settings
Use the MMC Snap-in GUI Instead of Normal GP Settings



Policy-Based Quality of Service

Policy-based quality of service (QoS) allows you to prioritize network traffic by setting a policy to throttle network traffic in favor of one protocol over another. In other words, you can specify that file transfer protocol (FTP) traffic use less available bandwidth than real-time streaming protocol (RTSP). Without QoS, ensuring that critical applications had the required bandwidth would have required purchasing more bandwidth in the form of additional hardware and cabling. QoS prioritizes network traffic by assigning a Differentiated Services Code Point (DSCP) value. And as described in request for comment (RFC) 2474, these values can range from 0 to 63, with the higher value getting the higher priority. For more information on RFC 2474, visit www.ietf.org/rfc/rfc2474.txt.

To manage the use of the network bandwidth, you configure a QoS policy, and make sure you specify a throttle rate, which is not selected by default. Follow the steps shown in Exercise 4.9 to create a QoS policy that will throttle the rate of transfer during a NetBIOS file copy to any file server in the organization.

EXERCISE 4.9

CONFIGURING A QoS POLICY

1. Create a new GPO or edit an existing one.
2. Expand to **Computer Configuration | Policies | Windows Settings | Security Settings | Policy-based QoS**.
3. Right-click **Policy-based QoS**, and then click **Create new policy**.
4. In the **Policy-based QoS** dialog box, on the **Create a QoS policy** page, in the **Policy name** field, give the policy a descriptive name, such as **File Transfer QoS Policy**.
5. In the **Specify DSCP Value** field, enter **63**. You may enter a number between 0 and 63, where the higher number takes priority.
6. Select **Specify Throttle Rate**, and enter **64Kbps** (or whatever rate you think is appropriate), and then click **Next**.
7. On the **This QoS policy applies to** page, select **All applications**, and then click **Next**. *NOTE* You can select a specific application by path and executable name.
8. On the **Specify the source and destination IP addresses** page, in the **This QoS policy applies to** field, select **Any source IP address**. *NOTE* On this page you can also select a specific IPv4 or IPv6 address instead.
9. In the **This QoS policy applies to** field, select **Any destination IP address** and then click **Next**. *NOTE* On this page you can also select a specific IPv4 or IPv6 address instead.
10. On the **Specify the protocol and port numbers** page, in the **Select the protocol this QoS policy applies to** field, select **TCP**.
11. In the **Specify the source port number** field, select **From any source port**.
12. In the **Specify this destination port number or range** field, select **To this destination port number or range**, then type **139**, and then click **Finish**.

Startup and Shutdown Scripts

We have learned that Group Policy does a background refresh every 90 minutes, by default, for workstations, and every five minutes by default on the domain controllers. However, startup scripts and shutdown scripts do not run during this background refresh. The startup scripts only run at startup, and the shutdown scripts only run at computer shutdown or reboot.

Unlike the logon and logoff scripts, which run under the user's credentials, startup and shutdown scripts run under the context of local system and, therefore, have full rights to all parts of the OS. In earlier versions of Windows, startup scripts were run synchronously. This means that they ran at startup, and would need to complete running prior to the user being allowed to log on. In Windows Vista and Windows Server 2008, the startup scripts run asynchronously, which means that the user can log on while the script continues to run in the background.

Creating a startup or shutdown script is the same process as creating a logon or logoff script. Expand **Computer Configuration | Policies | Windows Settings | Scripts**, select either **Startup** or **Shutdown**, and then follow the steps logon scripts, described in Exercise 4.7. See Figure 4.12.

Figure 4.12 Startup Script Which Will Install a Custom Application





TEST DAY TIP

If you use startup scripts to install software, Group Policy will begin the installation of the software but will not manage it after that. So the application will not be self-healing like other Group Policy software installation applications, and will not be uninstalled if the computer falls out of the scope of management. However, if you must install an application through an EXE or Office 2007 using the MSP file, you must use a script to install it.

Administrative Templates

As we have already discussed, the Administrative Template settings under Computer Configuration will modify a registry key in the hive **HKEY_LOCAL_MACHINE**. The benefit of using Administrative Templates to modify these keys is that you do not need to know the exact key. Simply set the settings and Group Policy refresh does the rest.

Just as in the user-side Administrative Templates, these template files are also written as ADMX/ADML files, and can be stored in a central store on the domain controller. The Computer Configuration Administrative Templates that can be set are:

- **Control Panel** Includes regional and language options, and user accounts
- **Network** Includes Background Intelligent Transfer Service (BITS), DNS Client, and offline files
- **Printers** Includes **Automatically publish new printers in Active Directory**
- **System** Includes Disk Quota, Kerberos, Power Management, and System Restore settings
- **Windows Components** Includes BitLocker Drive Encryption, Event Viewer, Security Center, and Windows Update settings
- **All Settings**

If you are unsure about what the settings mean that are defined by the Administrative Templates, go to the **Properties** dialog box of a particular setting, and click **Explain**. Each setting has an Explain tab.

GPO Templates

Windows Server 2008 and the Group Policy Management Console (GPMC) come with a new feature called *Starter GPOs*. These Group Policy Objects have specific Administrative Template settings that have already been enabled or disabled, and are used to create new GPOs that require these same settings, but also require other settings.

TEST DAY TIP

Other features that fall under the category of Group Policy templates are Administrative Templates, ADMX file Central Store, and Restricted Groups. All of these features have been previously described in detail.

Starter GPOs

As we have discussed, Starter GPOs provide the ability to store a collection of Administrative Template settings in a single GPO. Once created, you can import and export the Starter GPO, making it easy to distribute to other environments that require the same settings in their Group Policy Objects. To create a Starter GPO, log on as a user with rights to create GPOs or use the **runas** command, and then follow the steps listed in Exercise 4.10.

EXERCISE 4.10

CREATING A STARTER GPO

1. Launch Group Policy Management Console (GPMC).
2. Expand Forest: *your forest name* | Domains | *your domain name* | Starter GPOs.
3. Click Starter GPOs. *NOTE* If no Starter GPOs folder exists in the shared SYSVOL folder on the domain controller, then GPMC will display **Create Starter GPOs Folder** button. If the folder exists, this button will not be displayed.
4. In the Starter GPOs in the details pane of *your domain name*, click **Create Starter GPOs Folder**, if applicable.

5. Right-click **Starter GPOs**, and then click **New**.
 6. In the **New Starter GPO** dialog box, type a descriptive name and optional comment and then click **OK**.
 7. In the **Folders** pane, right-click **your new Starter GPO**, and then click **Edit**.
 8. In the **Group Policy Starter GPO Editor** box, configure the appropriate Computer Configuration and User Configuration Administrative Template settings, and then close this window.
-

When you are ready to create a new GPO using this Starter GPO as a template, simply right-click the **Starter GPO**, and then select **New GPO from Starter GPO**, and then configure the rest of the GPO settings.

Linking GPOs to Active Directory Objects

Earlier in the chapter we mentioned that Group Policy Objects can be linked to different containers within Active Directory. These containers are the site, domain, OU, or child OU. We also discussed that there is no mechanism for linking a GPO to the forest or to the default containers, such as Users or Computers. When you link a GPO to one of the containers listed here, that means that the settings within that GPO will apply to all of the computers or users within that site, domain, or OU, and only to those computers and users. In other words, if you create a GPO and link it to the Sales OU, the users and computers within the Accounting OU will not see those settings. However, because the GPOs can be linked to domain and to OUs, the possibility of a conflict arises, for example, when a GPO administrator links a GPO to the domain, but another GPO administrator links a GPO to the OU that has conflicting IE Maintenance settings. Which one of these settings will win?

In this section, we will describe how to create and link a GPO, and what happens in the case of a conflict. We will also discuss the Resultant Set of Policies (RSoP), using Windows PowerShell and the GPO hierarchy.

Linking GPOs

By linking GPOs, the GPO administrator is telling Active Directory which users or computers will receive these settings. GPOs that are linked to the site, for example, will be deployed to all computers within the IP subnets defined by the site. Because

the Active Directory site could conceivably span multiple domains, only the Enterprise Admin or a Domain Admin in the forest root domain can link a GPO to the site. Examples of settings that may have a site-wide application are virus scanning software and definitions, Group Policy Preferences defining an environment variable, or deploying a new printer. Keep in mind the settings that will not apply over a slow link, however, and plan the GPOs accordingly. For example, if you use Group Policy Preferences to map a drive, and that policy is linked to the site, and there is a slow link connecting the site to the nearest DC, then that policy setting will not be applied. For a list of other settings that may or may not be applied, see the section titled “Understanding Group Policy Preferences” in this chapter.

When you link a GPO to the domain, the settings will apply to all users and computers within that domain. In today’s Active Directory, it is more common to link GPOs to the organizational unit. If your domain spans multiple geographic locations, keep in mind the same rules will apply here in regards to processing GPOs over slow WAN links.

Finally, linking a GPO to the OU is the most common implementation. Designing the Active Directory Site infrastructure around GPO management is not practical; nor is designing the domain for this same reason. However, designing the OU structure for Group Policy is not only practical, but it is widely practiced. When you design your OUs, you must consider the fact that you will be using Group Policy in your organization. By linking GPOs to OUs, you are able to delegate control to the OU admin, and are able to departmentalize the application of GPOs to very specific sets of users and computers.

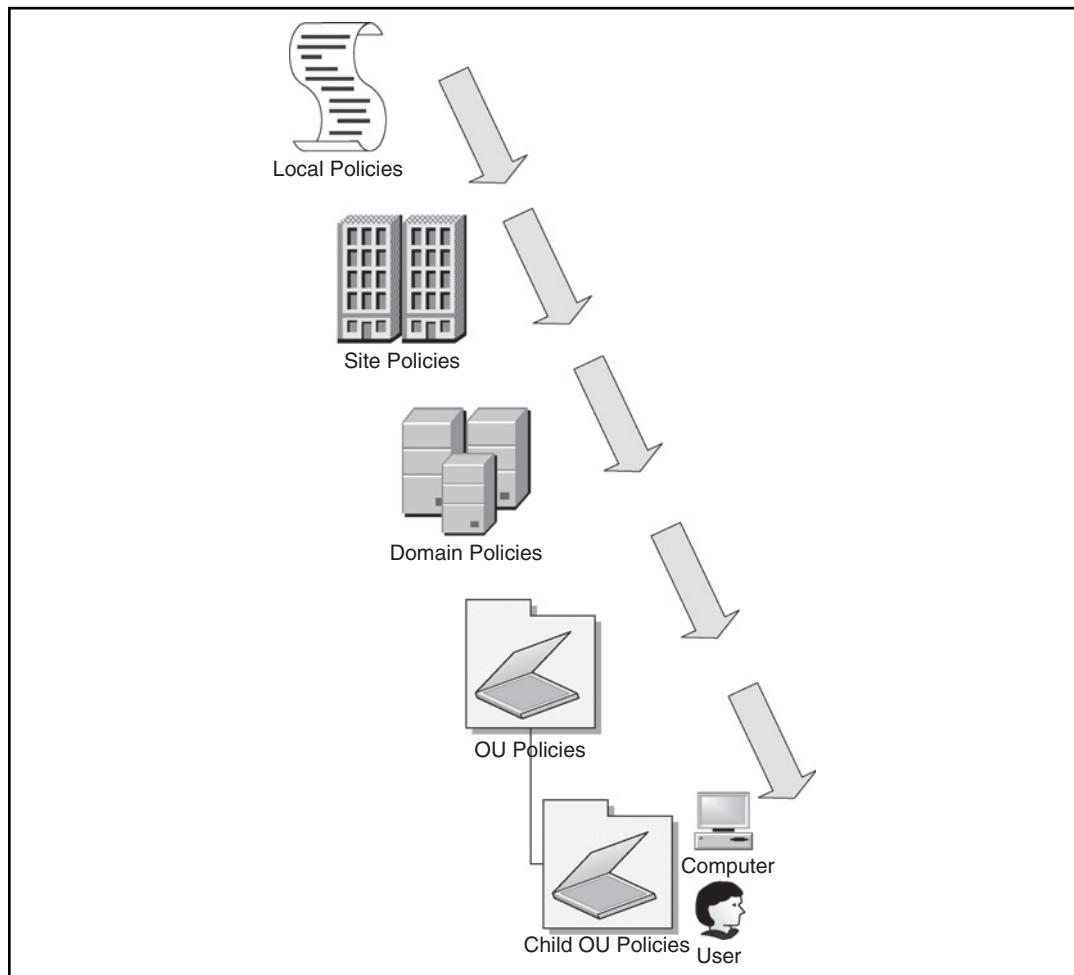
Group Policy Object Conflicts

All settings from all GPOs get applied at startup, logon, or the background refresh interval. This is without exception. However, you may notice that it appears as if one setting gets applied instead of another setting. This would be the result of a conflict of two or more GPOs that have the same setting set, but are set differently. For example, if one GPO enables **User Configuration | Policies | Administrative Templates | Start Menu and Task Bar**, but another GPO disables this same setting, both will be applied, but only one will win. Which one?

Group Policy Objects are applied in the following order: local policy, site, domain, OU, child OU, and so on. This means that upon startup, your computer will process all of the local Computer policies; then it will ask for all of the GPOs that have been linked to the site, and apply all of those policies, overwriting any policy setting from the local computer policy that might conflict. After those have

been applied, it asks for all of the GPOs that have been linked to the domain, and again will process them all, and overwrite any policy setting from the local computer policy or the site-level GPOs that conflict, and then the parent OU policies, the child OU policies, and so on, until all policies have been applied from all containers that are part of the computer's hierarchy. Once those have been applied, the user logs on, and the process starts all over again with the user-side settings. See Figure 4.13 for an example of how Group Policies apply.

Figure 4.13 Group Policy Processing Order

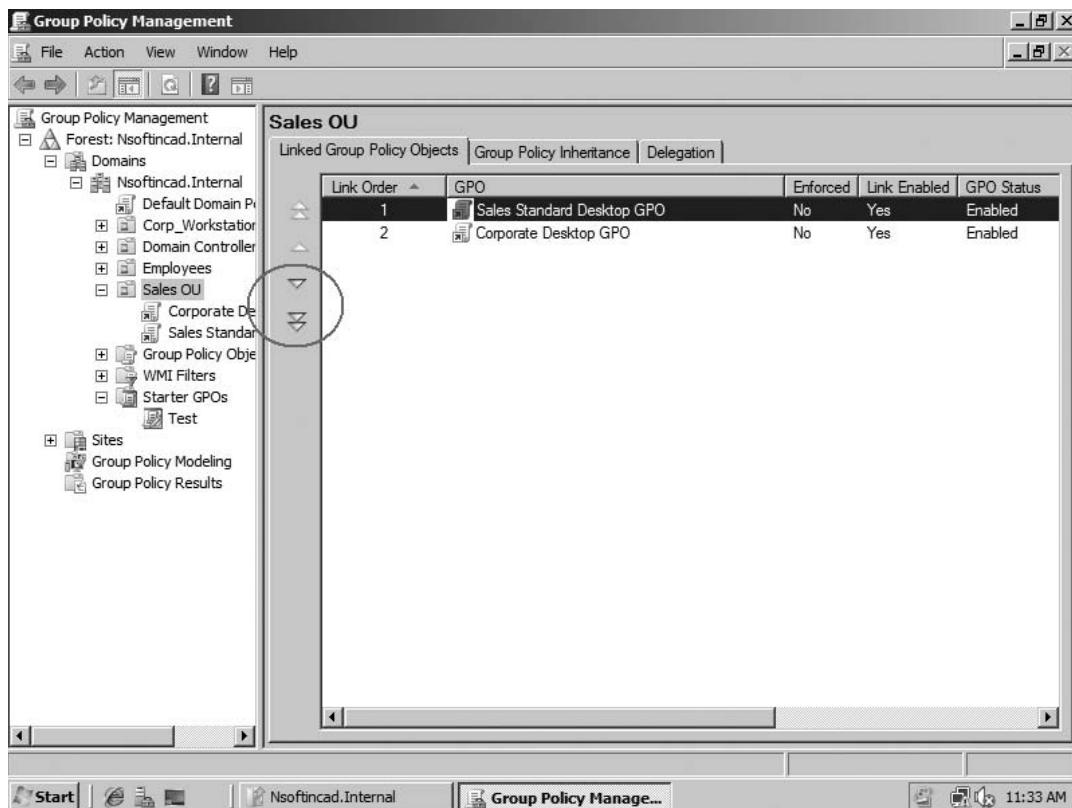


Using the example in Figure 4.13 and the example setting earlier about Lock the Taskbar, if this policy were enabled at the Domain level policies, yet an OU

admin at the child OU created a policy that disabled that setting, then the setting will be disabled, because that is the setting that applies last and is closest to the user.

Other setting conflicts may be caused by two or more group policies linked to the same container and having conflicting settings. Figure 4.14 shows what happens if these GPOs conflict. When GPOs from the same container are applied, they are applied from the bottom up. You use the arrows circled in Figure 4.14 to reorder the list of GPOs.

Figure 4.14 When GPOs Conflict



In Figure 4.14, when it is time to process the GPOs from the OU, the first one processed will be Corporate Desktop GPO, and then Sales Standard Desktop GPO. Any settings that conflict will be set by the Sales Standard Desktop GPO. If you would prefer that the settings from any other GPO be applied last, then you can reorder that list of GPOs by using the arrows on the left of the details pane.

Two other options that can be set when designing the Group Policies are **Enforced** and **Block Inheritance**. Setting **Enforced** on a Group Policy Object means that these settings will apply even if they are in direct conflict with another GPO that will be written after this one. It also means that if an OU administrator set **Block Inheritance** on the OU, then this GPO's settings will still be inherited. **Block Inheritance** means that no GPOs that have been defined at higher containers will be inherited down to this container, provided that the enforced attribute has not been set on a higher GPO. For example, if you need to set a policy that will affect all domain users except for those in the Sales OU, you might link the policy to the domain, and then set **Block Inheritance** on the Sales OU. However, this will block *all* GPOs and not just the one GPO. So use **Block Inheritance** very sparingly.

The best way to determine which policy settings have been set is by using Group Policy Results, also known as Resultant Set of Policies (RSoPs).

RSoP

As you can see from the above examples, it is possible, and likely, that you will set a Group Policy and notice that some of the settings may appear to have not been applied. That is probably because of the conflicting policies, and the fact that the last one written (applies) wins. If you would like to see a listing of all of the GPOs and their settings that have been applied, you can run either the command-line tool **gpresult.exe** use the Group Policy Results node within the GPMC console, or run **RSOP.msc**.

Using **gpresult.exe** is as easy as it sounds. Open a command prompt, type **gpresult /R**, and let it go. Of course there are other parameters that you can set with it, but if you use **/R** it will give you a report of the policy settings that have been applied to your user account while logged onto this workstation (see Figure 4.15). This report can be lengthy, depending on the number of GPOs applied. Notice **gpresult** will even check the speed of the link to the DC.

Figure 4.15 Gpresult Running the RSoP Report

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is "gpresult /R". The output displays the RSOP data for the user "NSOFTINCAD\Administrator" on the computer "ALPHA" in Logging Mode. It provides details about the OS configuration (Primary Domain Controller, Version 6.0.6001), site name (Default-First-Site-Name), roaming profile (N/A), local profile (C:\Users\Administrator), and connection status (Connected over a slow link? No). The "COMPUTER SETTINGS" section shows the domain controller (CN=ALPHA,OU=Domain Controllers,DC=Nsoftincad,DC=Internal), last policy application time (3/20/2008 at 3:00:33 PM), group policy slow link threshold (500 kbps), domain name (NSOFTINCAD), and domain type (Windows 2000). The "Applied Group Policy Objects" section lists the Default Domain Controllers Policy and Default Domain Policy. A note indicates that several GPOs were not applied due to filtering. The "The computer is a part of the following security groups" section lists BUILTIN\Administrators, Everyone, BUILTIN\Users, and BUILTIN\Pre-Windows 2000 Compatible Access.

```
C:\>gpresult /R
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 3/20/2008 at 3:03:59 PM

RSOP data for NSOFTINCAD\Administrator on ALPHA : Logging Mode

OS Configuration: Primary Domain Controller
OS Version: 6.0.6001
Site Name: Default-First-Site-Name
Roaming Profile: N/A
Local Profile: C:\Users\Administrator
Connected over a slow link?: No

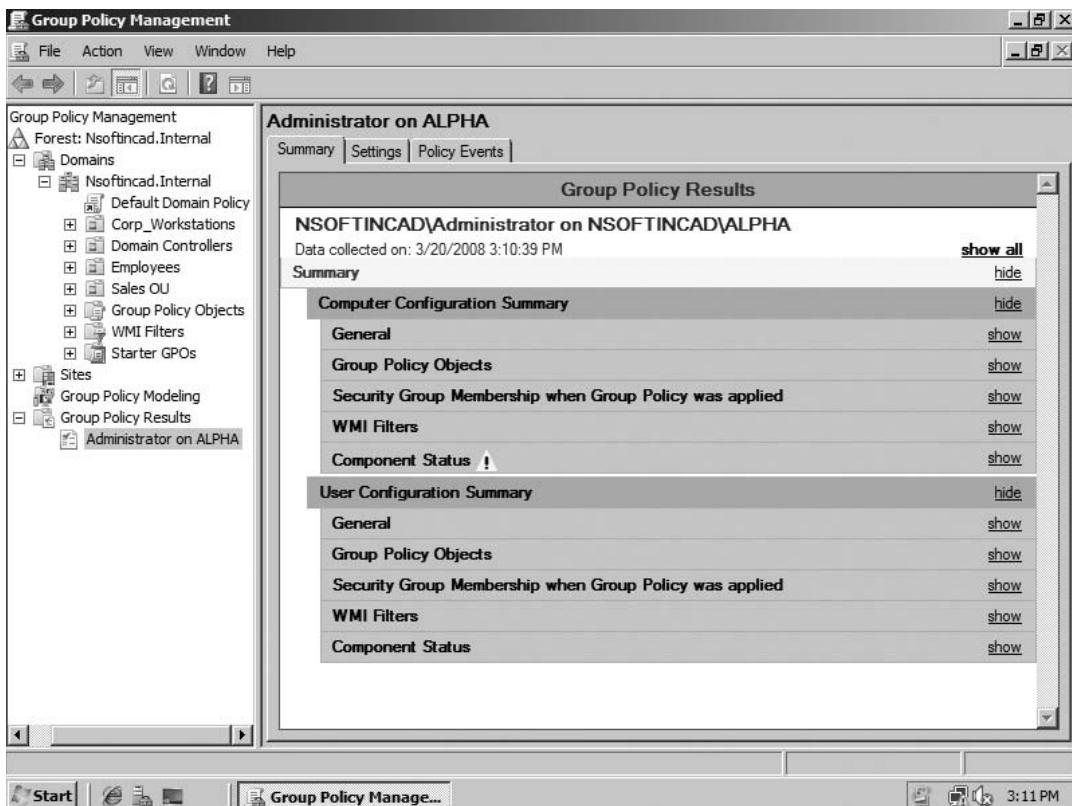
COMPUTER SETTINGS
CN=ALPHA,OU=Domain Controllers,DC=Nsoftincad,DC=Internal
Last time Group Policy was applied: 3/20/2008 at 3:00:33 PM
Group Policy was applied from: Alpha.Nsoftincad.Internal
Group Policy slow link threshold: 500 kbps
Domain Name: NSOFTINCAD
Domain Type: Windows 2000

Applied Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy

The following GPOs were not applied because they were filtered out
Local Group Policy
Filtering: Not Applied <Empty>

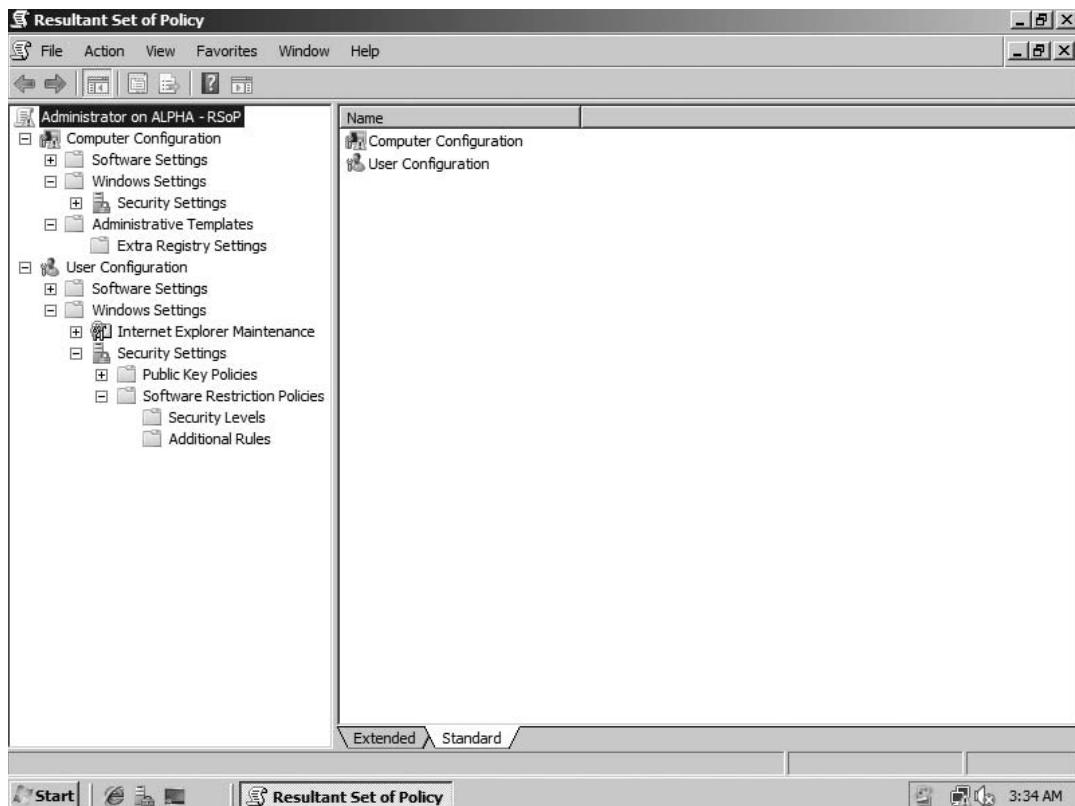
The computer is a part of the following security groups
BUILTIN\Administrators
Everyone
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
```

Using the GPMC might be easier for some of you, as it is wizard-based, and displays the information in an easy-to-view HTML page. This report can also be exported as XML. See Figure 4.16 for an example of the RSoP Wizard. In this figure, the component status shows a warning because a reboot is required for a setting to apply. Notice that this wizard will allow you to Show or Hide the specific settings that have been set, and if a reboot is required to apply a setting, a Warning icon will appear.

Figure 4.16 The Group Policy Results Wizard

RSoP.msc is a new MMC console snap-in that when called determines all of the settings that apply to your user account logged onto the workstation that you called the snap-in from, and displays it to you in a MMC console that looks like the Group Policy Management Editor. However, instead of showing you the hundreds of settings available in Group Policy, it only displays those that have been set by the local security policy and all GPOs that have been applied after log on and background refresh. See Figure 4.17. Note that if you open an MMC console and then add the snap-in Resultant Set of Policy, you will have to use the **Action** menu to run through the RSoP Wizard. If you call **RSoP.msc** from the **Run** menu, the wizard will run automatically in Logging mode, assuming the current user account on the current computer.

Figure 4.17 RSoP.msc Snap-in Displaying Only Those Policies That Have Been Applied



TEST DAY TIP

Do not get Group Policy Results confused with Group Policy Modeling. GP Modeling will allow you to see the results of Group Policy *before* moving a user or computer object into a new OU or *before* a user logs on. Group Policy Results will allow you to see the results of Group Policy *after* the user has been moved or logs on.

Managing Group Policy with Windows PowerShell

Windows PowerShell is a command-line scripting language which allows IT administrators to more easily administer and automate administrative tasks on their servers.

PowerShell is available on Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008 (except for Server Core installations), and includes more than 130 standard command-line tools, with a verb-noun syntax that makes it easier to learn and adopt into your environment. If you are using Exchange Server 2007 or System Center Virtual Machine Manager, you can use Windows PowerShell to improve efficiency and productivity.

Group Policy can also be managed by Windows PowerShell. Why use Windows PowerShell? When the GPMC was released several years ago, Microsoft made scripting possible to help GPO administrators automate tasks, such as backing up, moving, and linking GPOs. These scripts could be written in VB. However, because they were written in VB, an entire script would have to be run. Windows PowerShell gives administrators the ability to either run the entire PowerShell script, or line-by-line. Additionally, VB did not give us the opportunity to modify the settings within the GPO, only the properties of the GPO. Table 4.2 shows the available PowerShell commands (also known as cmdlets—pronounced command-let).

Table 4.2 List of Available Windows PowerShell Cmdlets for Managing GPOs

| Function Name | Description |
|--------------------|---|
| BackupAllGpos | Backs up all GPOs in the domain |
| BackupGpo | Backs up a specific GPO |
| RestoreAllGpos | Restores all GPOs from a backup to a domain |
| RestoreGpo | Restores a specific GPO from backup |
| GetAllBackedUpGpos | Retrieves the latest version of GPO backups from the path provided |
| CopyGpo | Copies all of the settings from one GPO to another |
| CreateGpo | Creates a GPO with no settings set |
| DeleteGpo | Deletes a specific GPO |
| FindDisabledGpos | Finds all GPOs with both the User and Computer Configurations settings disabled |
| FindUnlinkedGpos | Finds all GPOs that have been created, but not linked to any containers |
| CreateReportForGpo | Creates an XML report for a specific GPO in a domain |

Continued

Table 4.2 Continued. List of Available Windows PowerShell Cmdlets for Managing GPOs

| Function Name | Description |
|------------------------|--|
| CreateReportForAllGpos | Creates an XML report for each of the GPOs in a domain |
| GetGpoByNameOrID | Finds a GPO by its name or GPO ID |
| GetBackUpByNameOrID | Finds a GPO backup by its display name or GPO ID |
| GetAllGposInDomain | Finds all GPOs in a domain |

To use these cmdlets, Microsoft has written several VB scripts to make your life easier. These scripts are installed into the %programfiles%\Microsoft Group Policy\GPMC Sample Scripts directory. Note that if you are using the version of GPMC that came bundled with Windows Server 2008, you may need to download the sample scripts from Microsoft's download center. This is a free download and well worth doing. Use the Windows PowerShell commands shown in Exercise 4.11 to create a new GPO and see which GPOs have been modified in the last 24 hours.

EXERCISE 4.11

USING WINDOWS POWERSHELL TO CREATE A NEW GPO

1. Launch **Windows PowerShell**.
2. Type **\$gpm = New-Object -ComObject GPmgmt.GPM** and then press **Enter**.
3. Type **\$gpm | Get-Member** and then press **Enter**. *NOTE* This will display the properties and methods the object supports.
4. Type **\$gpmDomain = \$gpmGet.Domain("Nsoftincad.Internal", "", \$gpmConstants.UseAnyDC)** and then press **Enter**. *NOTE* This will instruct PowerShell to use any writeable DC to perform this operation.
5. Type **\$gpmNewGPO = \$gpmDomain.CreateGPO()** and then press **Enter**. *NOTE* This will instruct PowerShell to create a new GPO in the domain **nsoftincad.internal**.

6. Type **\$gpmNewGPODisplayName = "Sales GPO created with PS"** and then press **Enter**. **NOTE** This will name the new GPO “Sales GPO created with PS”.
 7. Type **\$gpmSearchCriteria = \$gpm.CreateSearchCriteria()** and then press **Enter**.
 8. Type **\$gpmAllGpos = \$gpmDomain.SearchGPOs(\$gpmSearchCriteria)** and then press **Enter**.
 9. Type **foreach (\$gpmGpo in \$gpmAllGpos) { if (\$gpmGpo.ModificationTime -ge (get-date).AddDays(-1)) {\$gpmGpo.DisplayName}}** and then press **Enter**.
-



NOTE

Steps 7 through 9 set the search criteria to search the domain listed above in Step 4, to list all GPOs that have been modified (or created) in the past 1 day (24 hours).

OU Hierarchy

As we have discussed earlier in the chapter, the design of your Group Policy will have an impact on the design of your organizational units (OUs). Linking GPOs to OUs is the most common implementation of Group Policy. This allows you to organize all of the computer and user accounts by department or job function, and give each the required software, registry keys, and other configuration settings necessary, without affecting other user accounts or computer accounts.

If you create an OU structure with parent and child OUs, consider the impact of the Group Policy processing order, as described in Figure 4.14. Because the GPOs set at the parent OU will apply before the settings in the GPOs linked to the child OU, the settings which are linked to the child OU GPOs will be written last and, therefore, will apply. Therefore, it is common to set broad policies at the parent OU, and then set more specific policies (but not conflicting policies) at the child OU. For more information on how to design your OU hierarchy, see Chapter 3.

Understanding Group Policy Hierarchy and Scope Filtering

Because of the nature of Group Policy and the order of processing, it is difficult to create a GPO that will apply to all of your users (except for a select few) without linking that GPO to the domain, adding those select users to their own OU, and then configuring the OU to **Block Inheritance**. The problem with this arrangement is that these users will now miss all of the other policy settings from all of the other GPOs that have been linked to the domain, or to the OUs that those users *should* be members of. Therefore, instead of segregating the users into different OUs, you should use filters on the GPOs to ensure that the correct users are getting the correct settings applied to them. In this section we will take a deeper look at Group Policy hierarchy and scope filtering.

Understanding Group Policy Hierarchies

We have already discussed the processing of GPOs as it relates to which container policies get applied first. We have also discussed using **Block Inheritance** and **Enforce** to ensure policies do not come down to a specific container or to ensure that they do. But let's dive into these topics a little deeper. Upon startup, all of the computer-based policies are written asynchronously with the startup processes. This means that the startup processes do not need to complete before the Group Policies start to apply. This makes startup quicker than in earlier versions of Windows. Once the local policies have been written and applied, the site-level policies are written; then the domain policies and the OU policies are written, writing all of the policies until the last policy is applied in the child OU that holds the Computer object in Active Directory. At logon, the same procedure happens with the user-side policies; these are also done asynchronously to speed up the logon process. If at any time during these processes **Enforce** has been selected, then that Group Policy and all of its settings will be applied to both the computer and user, even if there is a conflicting setting or if **Block Inheritance** has been selected on the OU. Let's look at the following example together:

- GPO-1 is linked to the Site and Installs Networking Application
- GPO-2 is linked to the Domain and has Standard Security settings and has **Enforced** selected
- GPO-3 is linked to the Domain and has Custom Desktop Configuration Settings applied

- GPO-4 is linked to the parent OU, has More Specific Desktop Configurations settings, and has **Block Inheritance** set
- GPO-5 is linked to the child OU and has Security settings set that are conflicting with GPO-2

If a computer and user account are both in the child OU, then GPO-2's security settings will apply, as will GPO-4. GPO-5 will not be applied even though it was written last because the settings in GPO-2 have been marked as **Enforced**. Without **Block Inheritance**, all GPOs will apply (except for GPO-5), and the Desktop Configuration Settings in GPO-3 will be set, and then any conflicting settings from GPO-4 will also be set.

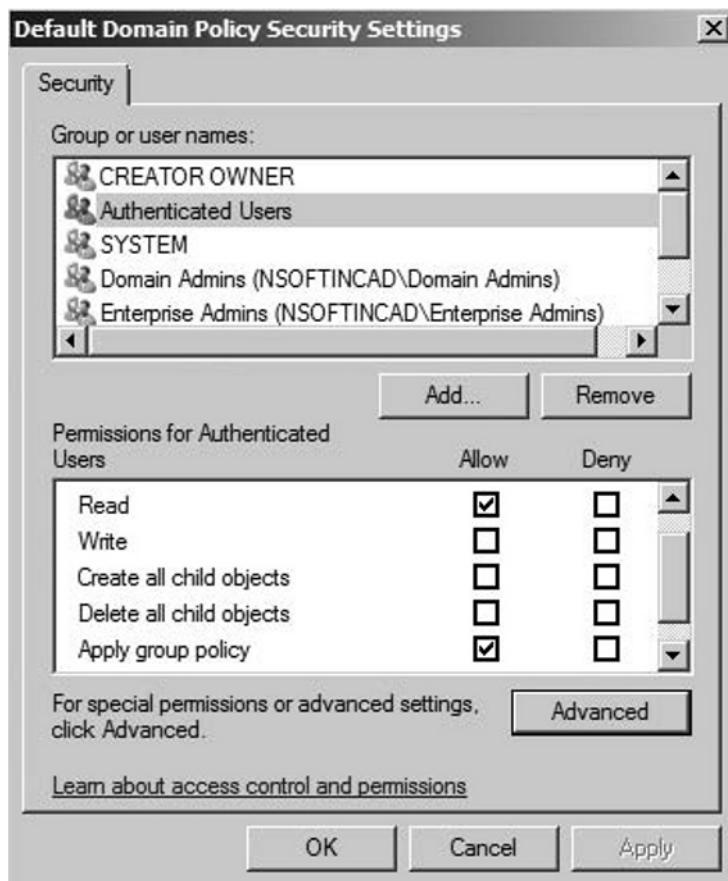
As we have said, use these settings sparingly. Overusing **Enforced** and **Block Inheritance** will lead to confusion on the part of your users, Help Desk staff, and GPO administrators.

Understanding Scope Filtering

Scope filtering is the process of excluding certain users or computers from receiving policy settings. Scope filtering can be in the form of Block Inheritance, as we discussed earlier, in the form of permissions, or by using WMI (Windows Management Instrumentation) filters. Regardless of the scope filtering process, **gpresult** and **RSoP** will look for these filters upon reading the applied Group Policy settings.

Scope Filtering: Permissions

By default, all users have two permissions set on all GPOs in the domain: Read and Apply group policy permissions. The Read group policy permission allows for **gpresult.exe** and **RSoP** to let the user know which settings have been applied. Without the Read group policy permission, the settings would apply, but the user would be unable to run a report on these settings or view which settings have been applied to them. The Apply group policy is the permission that actually allows the policy to be written to the user or computer. See Figure 4.18 for the permissions to the Default Domain Policy Security setting. Note that Full Control and Special permissions are not visible in the figure due to resolution. Authenticated users have to apply group policy.

Figure 4.18 Default Permissions on the Default Domain Policy

The default permissions on all GPOs—Domain Admins, Enterprise Admins, and System—have Full Control but do not have Apply group policy. Authenticated Users have Read and Apply group policy. The Authenticated Users group includes all computers that have started and connected to the domain and all users who have successfully logged on, including members of the Domain Admins and Enterprise Admins groups. By setting the permission Apply group policy to **Deny** for the security group you wish to exclude from receiving the settings, you are ensuring that these policy settings do not apply to users of this group. This is more efficient than moving those users into their own OU. And because these are NTFS permissions, the **Deny** permission takes precedence over the **Allow** permission.

Scope Filtering: WMI Filters

WMI is Microsoft's implementation of WBEM, or Web-Based Enterprise Management. Using WMI, administrators are able to create queries against a computer to determine hardware configurations such as RAM, CPU, available disk space, print spooler configurations, and so on. WMI can also read certain software configurations, such as registry settings, network configuration settings, application settings, and so on. System Center Configuration Manager (SCCM 2007) uses WMI during its normal operation to collect inventory data for SCCM administrators. The GPMC can also use WMI to ensure that computers only get these policy settings if the appropriate configuration has been set. For example, a WMI Filter can be written and linked to a GPO that will install Microsoft Office 2007. You can create a GPO that will install Microsoft Office 2007, link it to the domain, and ensure that only computers that have 1 GB of RAM and at least 10 GB of free space on the hard drive will apply this GPO. Without WMI Filters you would have to use a third-party inventory tool to determine which computers meet the hardware restrictions, add those computers to a security group, and then select the **Deny Apply group policy** permission to that security group. Upon adding RAM or freeing up disk space, you would need to remove that computer from the security group to ensure it applied this policy. This process has a wide margin of error, as you have to wait until the next inventory process (typically once a week) runs and is examined to remove this computer from that security group. By using WMI Filters, the policy will apply as soon as you upgrade the hardware and turn the computer on (assuming the computer is turned off during the hardware upgrade, which recommended is for obvious reasons).

In our example, both queries would have to come back as true, showing at least 1 GB of RAM and 10 of GB free space on the hard drive. If either query returns a value of false, then the policy will not apply. Also, the WMI Filter is separate from the GPO. That is, the WMI query (written in WMI query language, called WQL) can be written once and linked to multiple GPOs. Your Windows 2000 workstations will not apply WMI Filters, however, during the processing phase of GPOs. So these computers will attempt to apply the policy even if they do not meet the appropriate conditions.

To create a WMI Filter that will evaluate the workstation for at least 1 GB of RAM and 10GB of free space on the hard drive, and to link it the filter to a GPO that is called Installs Microsoft Office 2007 GPO, follow the steps listed in Exercise 4.12.

Note that this exercise assumes a GPO has already been created and that this GPO has already been linked to the domain:

EXERCISE 4.12

CREATING A WMI FILTER

1. Launch **GPMC**.
2. Expand to Forest: *your forest name* | Domains | *your domain name* | **WMI Filters**.
3. Right-click **WMI Filters** and then click **New**.
4. In the **New WMI Filter** dialog box, in the **Name** field, type **Evaluate_RAM_HDD**.
5. In the **Description** field, type an optional description.
6. In the **Queries** field, click **Add**.
7. In the **WMI Query** dialog box, in the **Namespace** field, ensure **root\CIMv2** is populated. Otherwise, click **Browse** and browse for this local namespace.
8. In the **Query** field, type **SELECT * FROM Win32_LogicalMemory Configuration WHERE TotalPhysicalMemory > 1000000** and then click **OK**. *NOTE* If you incorrectly type this query, a message will pop up indicating that the query syntax is incorrect.
9. In the **Queries** field, click **Add**.
10. In the **WMI Query** dialog box, in the **Namespace** field, ensure **root\CIMv2** is populated. Otherwise, click **Browse** and browse for this local namespace.
11. In the **Query** field, type **Select * from Win32_LogicalDisk where FreeSpace > 10000** and then click **OK**.
12. In the **New WMI Filter** dialog box click **Save**.
13. In the GPMC, expand Group Policy Objects and then click **Installs Microsoft Office 2007 GPO**.
14. In the **WMI Filtering** section under **This GPO is linked to the following WMI filter**, select **Evaluate_RAM_HDD**.
15. In the **Group Policy Management** confirmation message box, click **Yes**. *NOTE* Each GPO can have only one WMI Filter linked to it.



TEST DAY TIP

Even though a single WMI Filter may be linked to one or more GPOs, each GPO can have no more than one Filter linked to it at a time. If you need to link more than one WMI Filter, consider creating a new filter with the combined settings of each of the other filters.

Controlling Device Installation

Controlling Device Installation via Group Policy is an option for those administrators who wish to control the usage of devices on the network, such as removable USB drives and other drivers. Using GPO, you can control the installation of a specific device or even a class of devices. It is also possible to control the access the user has once a device has been installed; for example, marking a USB port as read-only to prevent your users from copying data from the network onto their USB drives while still allowing them to read that data that is stored on the drive. This control can be marked as a computer-based policy; that is, it will apply to the computer regardless of who logs onto it, such as a public computer in your lobby; or it can be marked as a user-based policy so that it applies to a specific user or group of users regardless of where they log on.

Controlling Device Installation by Computer

When you set these policies settings at the Computer Configuration Administrative Templates, these settings will apply to all users who log on. However, to make sure administrators can override this policy, there is a setting called **Allow administrators to override Device Installation Restriction policies**. This will allow any user that is a local administrator on their workstation to override whatever other device installation polices you have set. Other settings that can be set at the Computer Configuration are:

- Allow installation of devices using drivers that match these device setup classes
- Prevent installation of devices using drivers that match these device setup classes
- Display a custom message when installation is prevented by policy (balloon text)

- Display a custom message when installation is prevented by policy (balloon title)
- Allow installation of devices that match any of these device IDs
- Prevent installation of devices that match any of these device IDs
- Prevent installation of removable devices
- Prevent installation of devices not described by any other policy setting

Allowing/Preventing Installation of Devices Using Drivers That Match These Device Setup Classes

When Windows detects that a new device has been attached to the computer, it queries the device for identification strings, which have been assigned by the hardware manufacturer. These identification strings are typically found in an IVF file, which is part of the driver package. Device setup classes are one of these identification strings. For example, all Bluetooth devices belong to the setup class Bluetooth, and all Network Adapters belong to the setup class Net.

When you use device setup classes to either allow or prevent users from installing devices, you must specify the GUID (Globally Unique Identifier). If you are installing a multifunction device, for example, an all-in-one printer, there will be multiple-device setup classes, one for each function.

Display a Custom Message When Installation Is Prevented by Policy (Balloon Text/Title)

When a device fails to install because of a Group Policy setting, this policy setting will pop up a dialog box with the title bar and message box populated with the settings defined here. If these settings are disabled or not configured, then a default message will be displayed.

Allowing/Preventing Installation of Devices That Match Any of These Device IDs

These settings specify a list of PnP (plug-n-play) hardware IDs that describe devices that users are allowed to or prevented from installing. When the **Allow** setting is enabled, users can install any PnP device that matches the ID of any device not listed in the Prevent policy. If any other policy settings in any other policies prevent a device ID from installing, that policy setting will take precedence over this **Allow** setting.

Preventing Installation of Removable Devices

When this setting has been applied, no new removable devices can be installed, and any removable device that has already been installed will not be able to update its driver.

Preventing Installation of Devices Not Described by Any Other Policy Setting

It would not be possible for any administrator to know the device ID of every single device that is currently available or that ever will be available. Therefore, this setting allows the administrator to prevent all of those hardware IDs without specifying them. If the device ID is not specified under the setting **Allow installation of devices that match these device IDs**, then this device cannot be installed or have its driver updated if it had been installed previously.

NOTE

Use caution when setting these policies. If you decide to use BitLocker Drive Encryption and have the key written to a USB device, you cannot prevent data being written to that USB device, or the operation will fail.

Controlling Device Installation by User

It is important to understand that the Device Installation policies are set at the Computer Configuration node in Group Policy. They are not set at the User Configuration and, therefore, take affect regardless of who is logged on. The only setting that looks for the logged on user is **Allow administrators to override Device Installation Restriction policies**. This policy checks to make sure the logged-on user is a member of a group with administrator rights on the workstation.

Summary of Exam Objectives

Group Policy allows administrators to configure and manage all of the user and computers in their environment without touching each and every machine. By using Group Policy, you can install software, add or remove registry keys, ensure security, control device installation, and so on. Because Group Policies can be linked to the Active Directory site, domain, OU, or even a child OU, it is often difficult to decipher these policies and exactly which settings have been applied. Therefore, through the Group Policy Management Console (GPMC) you can use Group Policy Results to get an HTML report of all of the settings that have been applied, or you can use the command-line tool **gpresult.exe**.

Besides for linking these GPOs to the Active Directory containers listed above, you can also filter them from being applied to security groups by using permissions or by using WMI Filters. These filters are written in WQL (the WBEM Query Language), and can be linked to one or more GPOs. Just remember that each GPO can only have one filter linked to it at a time.

Finally, we discussed controlling device installation using Group Policy. There are several settings that can apply to this topic, so make sure you understand each. Also, remember that these are all Computer Configuration policies. There are no Device Installation settings listed under User Configuration. However, the setting **Allow administrators to override device installation restriction policies** can be set to check the currently logged on user to see if he or she is an administrator on the local computer. If he or she is, then the restriction will not apply, assuming this policy has been enabled.

Exam Objectives Fast Track

Understanding Group Policy Preferences

- Linking GPOs to Active Directory Objects
- Understanding Group Policy Hierarchy and Scope Filtering
- Controlling Device Installation

Understanding Group Policy Preferences

- Group Policies now include Preferences, or settings that will apply but the user may override.
- Windows Server 2008 Group Policies use XML-based Administrative Templates, which can be stored in a central location.

- The default locations for new User and Computer objects can be redirected to OUs instead of the default containers so that these objects can get Group Policy settings applied immediately.
- You can change the preferred domain controller that processes GPOs. The default is the PDC Emulator.
- If Group Policy processing is happening over a slow WAN link, certain settings will not apply, while others will apply regardless of the speed of the link.
- GPMC gives the GPO administrator the ability to backup, restore, import, and export GPOs.
- Windows Server 2008 now comes with Starter GPOs, which are GPOs that contain some settings that another GPO will need and are used as a template for creating new GPOs.

Linking GPOs to Active Directory Objects

- GPOs can be linked to Active Directory sites, domains, OUs, and child OUs, but not to the default AD containers.
- GPOs are processed in a certain order; when one GPO is processed, if another GPO has any conflicting settings, the last GPO written (applied) wins.
- RSoP (Resultant Set of Policies) will help you determine which settings have been applied to a user based on the user's name and the computer he or she is logged onto.
- Windows PowerShell can be used to help you administer and link GPOs.

Understanding Group Policy Hierarchy and Scope Filtering

- You can use Block Inheritance on any part of the GPO hierarchy to block all GPOs from coming down to that container. This setting blocks all GPOs, not a specific GPO.
- You can use Enforce on any GPO that must have its settings applied, even if there is a conflicting GPO or if Block Inheritance has been set.

- WMI Filters offer a way to block Group Policy processing on specific computers by running a query on those computers first for specific amount of RAM, or hot-fix installed, and so on.
- WMI Filters can be applied to one or more GPOs. GPOs can have zero or one WMI Filter applied.

Controlling Device Installation

- Group Policy can be used to prevent your users from installing or using USB devices on their computers.
- USB ports can be marked as read-only so that users can read the files on the USB drives, but cannot write files to the USB drive.
- All Device Installation Group Policy settings are set at the Computer Configuration section of Group Policy.
- There is a setting that allows administrators to ignore the Device Installation restriction settings.

Exam Objectives

Frequently Asked Questions

Q: Can Group Policy be used to install all software applications?

A: Yes and No. By using the Software Installation node in Group Policy, only an MSI can be launched to install an application. However, through startup and logon scripts, you can write VB scripts that will launch the EXE with the proper settings, provided the VB script has already written.

Q: If I use a logon script to install software, will that software be managed by Group Policy the same as if I used an MSI and the Software Installation node?

A: No. If you use a logon script to install the software, then the software will not be self-healing like an MSI, and if the computer falls out of the scope of the Group Policy Object (for example, it gets moved into a different OU), then the software will not be able to uninstall.

Q: Do my users have to restart their computers every time I create a new GPO?

A: No. Most Group Policy settings which have been set at the Computer Configuration will set during the background refresh, which is every 90 minutes, by default. However, there are some security settings and software installation settings which do require a startup to take place. If the computers do not restart, then those specific settings will not apply.

Q: I did not receive all of the policy settings that I expected to receive when I restarted my computer and logged on. I do not have GPMC installed on my computer. How can I see which policies have been applied to me when I restart my computer and log on?

A: You can use the command-line tool **gpresult.exe**. Use the **/R** parameter. This will send a report to your command prompt window with all of the policies that applied, all of your user groups (for filtering information), any WMI Filters applied, and any GPOs that failed to apply and the reason for their failure. To save this report, use the **/H** parameter and specify a path where you want to save the HTML report.

Q: I need to create a GPO that will apply to all of my users when they log onto the network using laptops. If they log on from their desktops, I do not want the policy applied. Is this possible in Group Policy?

A: Yes. The most efficient way to accomplish this would be through a WMI Filter. Use the following syntax on the filter: **SELECT * FROM Win32_SystemEnclosure WHERE SystemEnclosure=9.**

Self Test

1. You are the Group Policy administrator for your company. The users in your accounting department need to have a custom application installed. You have contacted the vendor and they have supplied you with an MSI installation file. All of the users in your accounting department and their computer objects are in the Accounting OU. Each member must decide when the application gets installed. For security purposes, you do not allow these users to access Control Panel. How should you configure the Group Policy?
 - A. Link the GPO to the Accounting OU. Publish the Application to the Users group.
 - B. Link the GPO to the Accounting OU. Assign the Application to the Users group.
 - C. Link the GPO to the Accounting OU. Assign the Application to the Computers group.
 - D. Link the GPO to the Accounting OU. Assign a startup script that will install the application to the Computers group.
2. You are the Group Policy administrator for your company. All of the user accounts get created in the Users container and then get moved into their appropriate containers. You need to ensure that upon the creation of a new user account, it immediately receives a GPO called New Employee GPO; but other employees do not receive the settings from this GPO. How should you configure your environment?
 - A. Create an OU called New_Employees. Create a GPO called New Employees GPO and link it to the New_Employees OU. Run the **redirusr** command to redirect all new user accounts to the New_Employees OU.
 - B. Create an OU called New_Employees. Create a GPO called New Employees GPO and link it to the New_Employees OU. Run the **redircmp** command to redirect all new computer accounts to the New_Employees OU.
 - C. Create an OU called New-Employees. Create a GPO called New Employees GPO and link it to the domain. In the attributes of the GPO, select **Enforced**.
 - D. Create a GPO called New Employees GPO. Create a global security group called New Employees. Add all new employees to the global security

group. In the Delegation tab of the GPO, accept all default entries and then add New Employees security group with the Apply group policy permission set to **Allow**. Link the GPO to the domain.

3. You have been asked to create a Group Policy Object to be used as a template for other Group Policy Objects. What is the best way to create this GPO with the least amount of administrative effort?
 - A. Create a GPO and configure all appropriate settings. Use the GPMC to create an HTML report of the settings. For each new GPO, refer to this HTML report and reconfigure these same settings.
 - B. Create a GPO and configure all appropriate settings. Use GPMC to back up the GPO. For each new GPO, start by restoring the GPO and continuing from there.
 - C. Create a Starter GPO and configure all appropriate settings. For each new GPO, select the Starter GPO.
 - D. Create an Administrative Template (ADMX file). For each new GPO, import the ADMX file into the new GPO.
4. You are the Group Policy administrator for your company. Your company has a single forest with three domains, located in the U.S. and Canada. The company is headquartered in Toronto and has members from all domains in the Toronto office. You have been asked to create a Group Policy Object that will apply to only the computers in the Toronto location. You have ensured that your user account is in the Enterprise Admins group, as well as the Domain Admins group is in the forest root domain. How should you configure this GPO?
 - A. Create a GPO with the required settings and link it to the Toronto site.
 - B. Create a GPO with the required settings and link it to all of the domains.
 - C. Create a GPO with the required settings and link it to the Domain Controllers OU in the forest root domain.
 - D. Create a GPO with the required settings and link it to the Domain Controllers OU in each of the domains.
5. You are the Group Policy administrator for your company. Your company has locations throughout the U.S. and Canada and is setup as a single domain. You want to ensure that Group Policies can be created by administrators in each geographic location and processed by the clients in each location without

requiring the sending of traffic over the WAN. Which Administrative Template setting should you configure?

- A. Computer Configuration-Group Policy Slow Link Detection, enabled to 500 Kbps.
 - B. User Configuration-Group Policy Slow Link Detection, enabled to 500 Kbps.
 - C. Computer Configuration-Environment Policy Processing, enabled to **Allow processing across a slow network connection.**
 - D. User Configuration-Group Policy Domain Controller Selection.
6. You have just logged onto your workstation and noticed several policies that have been applied. You want to see which policies have been applied and then save the report as HTML. What are two ways to accomplish this? (Choose two answers. Each answer represents a complete solution.)
- A. Use **gpresult /R /H** and add the path to where you want to save the report.
 - B. Use the GPMC and Group Policy Modeling Wizard.
 - C. Use the GPMC and Group Policy Results Wizard.
 - D. Use **gpupdate /force >c:\gpo.htm**.
7. You are the Group Policy administrator for your domain and have been tasked with creating a policy that will apply to all of the computers in your domain, except for those computers in the Accounting OU, and including the computers in the Computers container. The computers in the Accounting OU should still receive all of the settings from the Default Domain Policy. How can you design your Group Policy infrastructure to allow the GPO to apply to all computers except for those in the Accounting OU while allowing the settings from the Default Domain Policy to apply to the specified computers?
- A. Link the new GPO to each of the OUs except for the Accounting OU. On the Default Domain Policy, select **Enforced**.
 - B. Link the new GPO to the Accounting OU. On the Accounting OU, select **Block Inheritance**. On the Default Domain Policy, select **Enforced**.
 - C. Link the new GPO to the domain. On the Accounting OU, select **Block Inheritance**. On the Default Domain Policy, ensure Authenticated Users have **Read** and **Apply** group policy permissions.

- D. Link the new GPO to the domain. On the Accounting OU, select **Block Inheritance**. On the Default Domain Policy, select **Enforced**.
8. You are the administrator of a Windows Server 2008 Active Directory forest. You have a single domain in a single location. You want to use scripting to manage your Group Policy Objects, including creating new objects, backing up and restoring GPOs, and creating reports for the GPOs. What tool should you use for this?
- Windows Command Prompt. Use **gpresult.exe**.
 - Windows Command Prompt. Use **gpupdate.exe**.
 - Windows PowerShell.
 - Group Policy startup scripts.
9. You are the administrator for your company's Windows Server 2008 Active Directory domain. You have designed the OU infrastructure so that each department has its own OU, with a child OU for the Users group and another child OU for the Computers group, with the appropriate objects placed into the appropriate OUs. You have decided to let the department managers link GPOs to their OUs as they feel are necessary. What should you do to allow the department managers to link the GPOs to their own OUs without allowing them to link GPOs to other OUs?
- Use the Delegation of Control Wizard on each OU. Delegate Generate Resultant Set of Policy (Planning) to the department managers.
 - Use the Delegation of Control Wizard on each OU. Delegate Generate Resultant Set of Policy (Logging) to the department managers.
 - Use the Delegation of Control Wizard at the domain. Delegate Manage Group Policy links to the department managers.
 - Use the Delegation of Control Wizard at each OU. Delegate Manage Group Policy links to the department managers.
10. You are the Group Policy administrator for your company's Active Directory domain. You have been assigned the task of creating a Standard Desktop for users in the sales department, which are spread throughout the U.S. and Canada. These users must all have the same security settings and applications installed on their desktops. These applications should only get installed on the computers in the sales department. What is the most efficient method for achieving this?

- A. Put all users from the sales department into the same OU. Create and link a GPO to this OU that will configure all of the settings and install the appropriate applications. Mark the GPO as **Enforced**.
- B. Put all users from the sales department into the Users container. Create and link a GPO to the domain that will configure all of the settings and install the appropriate applications. Mark the GPO as **Enforced**.
- C. Put all users from the sales department into the same IP subnet. Create and link a GPO to the site containing this IP subnet that will configure all of the settings and install the appropriate applications.
- D. Put all users from the sales department into the same OU. Create and link a GPO to the domain that will configure all of the settings and install the appropriate applications. Ensure the users from the sales department have Read and Apply group policy permissions. Configure the OU to **Block Inheritance**.

Self Test Quick Answer Key

- | | |
|-------------|----------------|
| 1. B | 6. A, C |
| 2. A | 7. D |
| 3. C | 8. C |
| 4. A | 9. D |
| 5. D | 10. A |

This page intentionally left blank

Chapter 5

MCITP Exam 647

Designing Identity and Access Management

Exam objectives in this chapter:

- Planning for Migrations, Upgrades, and Restructuring
- Planning for Interoperability

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

Sooner or later, IT departments face the challenge of whether to upgrade or restructure their environment. Be it a new operating system version or software that's mission critical, the infrastructure must support the new component. Infrastructures that grew over time are often very inflexible and do not fit the requirements of new operating systems or software programs. If the existing infrastructure is not appropriate for the implementation of the new software, a company might consider a migration or a restructure. Another example is mergers and acquisitions or a company split. In this chapter you will learn how to assess the requirements for an upgrade, a migration, and a restructuring of a Windows Server environment. We talk about the tools and techniques that exist and how to plan for their usage.

The future will bring even more challenges for IT departments, stretching the boundary of the internal network. So that applications and services are accessible for anyone, at any time, from any platform, specifically Business to Business (B2B) and Business to Customer (B2C) solutions. It is obvious that such infrastructures need additional security measures. How do you ensure the integrity of your data while a user connects from outside your company?

A completely new approach is delivering software over the Internet. Called Software as a Service (SaaS), it combines the flexibility of a hosted solution with the strength of rich applications. Companies with limited budgetary or personnel resources especially benefit from a SaaS solutions. By leveraging SaaS, these companies do not have to maintain certain applications or worry about licensing costs for these applications. Instead, they "rent" these services from an application service provider (ASP).

Interoperability between different platforms is another important part of finding a solution, which needs to be built on standards that are (theoretically) available on any system. Today, Web Services are the state-of-the-art technology to interoperate across platforms. They are built on top of the HTTP protocol standard that is widely adopted. Also known as WS-* specifications, Web Services define protocols for authentication, trusts, management, and more. We will have a look at these specifications in this chapter.

We should not forget the management aspect. Implementing an authentication and authorization solution that is open to entities outside the company normally also involves managing new identities, permission, and more. In large enterprises, you would have to plan for additional staffing and so on to manage such a solution. To lower the management overhead, companies can leverage Web Service to

implement federation. In a federation scenario, the company that offers a service only has to manage permissions. The company that accesses the service manages identities. With Windows Server 2008 Active Directory Federation Services (ADFS), you can implement such a solution. This chapter talks about the components of ADFS, their installation, and their configuration.

Finally, we show you which interoperability technologies Windows Server 2008 has to offer. We cover Services for Network File Service (formerly known as Services for UNIX) as well as application authentication and integration into Active Directory Lightweight Directory Services.

Planning for Migration, Upgrades, and Restructuring

A change in your IT environment should always be driven by the needs of the business. Thus, when you begin with your evaluation of the migration process, the first thing to do is to focus on the business reasons that caused you to consider a migration.

Business needs may be driven by a number of factors, including the need for more reliability, a more secure environment, or even implementation of a fault-tolerant service such as messaging. Another frequent reason for operating system upgrades is that the business needs to upgrade an application or install a newer version of an application, and that version only installs on the newer version of the operating system.

Software and hardware products also have a support cycle that will end at some point. The decision to upgrade is often triggered by the end of a product support cycle, even if your environment runs without any incidents. Before you upgrade, you should assess the risks that potentially result from an upgrade by comparing the losses that could occur when the support is unavailable, to the benefits from upgrading.

Knowing When to Migrate or Upgrade

When we talk about an update to a newer operating system version on a domain controller, we always talk about a *migration*. This might be confusing in the beginning, but if you think about it, it will make sense. When you migrate your existing Active Directory infrastructure by introducing Windows Server 2008 domain controllers, you *upgrade* the directory service to a new version. The topology does not change during an upgrade. When you migrate or restructure, you *migrate* existing objects to a *new* directory service. Thus, the topology changes during

a restructuring. Two scenarios exist for restructuring: intra-forest and inter-forest. As we heard before, the decision to upgrade or migrate/restructure your directory service infrastructure is influenced by many factors.

Backward Compatibility

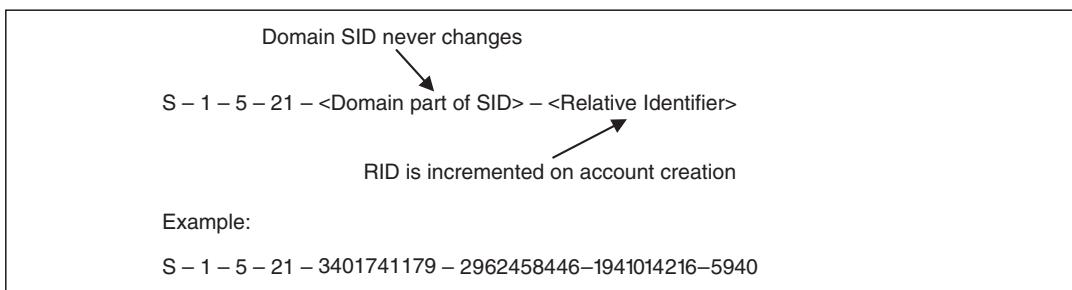
Whether you use the migration or the upgrade method, maintaining compatibility with older systems is a key requirement. Most customers I'm involved with operate heterogeneous networks where Microsoft products often build the basis for directory services, but other services, like file and print, are served by other operating systems. A classic example is the use of SAMBA. SAMBA is an open source implementation of the Microsoft Server Message Blocks (SMB) protocol that runs Unix-based systems. It provides Windows file sharing capabilities to clients. Another functionality of SAMBA is that it can serve as a NT4-Style domain controller. If you use the file sharing component of SAMBA, a migration to Windows Server 2008 might break this functionality because of tightened security settings in Windows Server 2008.

Another factor when it comes to backward compatibility is supporting client operating systems other than Windows. Good examples are Apple Macintosh computers. In Windows Server 2003, you could install File and Print Services for Macintosh to serve these clients. In Windows Server 2008, this component no longer exists. An alternative is the SAMBA client, which the Mac operating system offers by default. However, having a large population of Macintosh clients requires careful planning to reconfigure these systems in a timely manner.

You also need to plan for legacy Windows operating systems such as Windows 98 or Windows NT4. Because of their poor system security, Windows Server 2008 Active Directory no longer supports those systems. A possible solution would be to upgrade those systems or to replace them completely.

Object Migration

You have learned that a unique number, called the Security Identifier (SID), identifies users and groups (called security principals) on a Windows system or in an Active Directory. The SID is a 32-bit number that consists of a domain part and a relative identifier (RID). A SID is eliminated during object deletion and is never reused. Figure 5.1 shows the structure of a SID.

Figure 5.1 SID Components

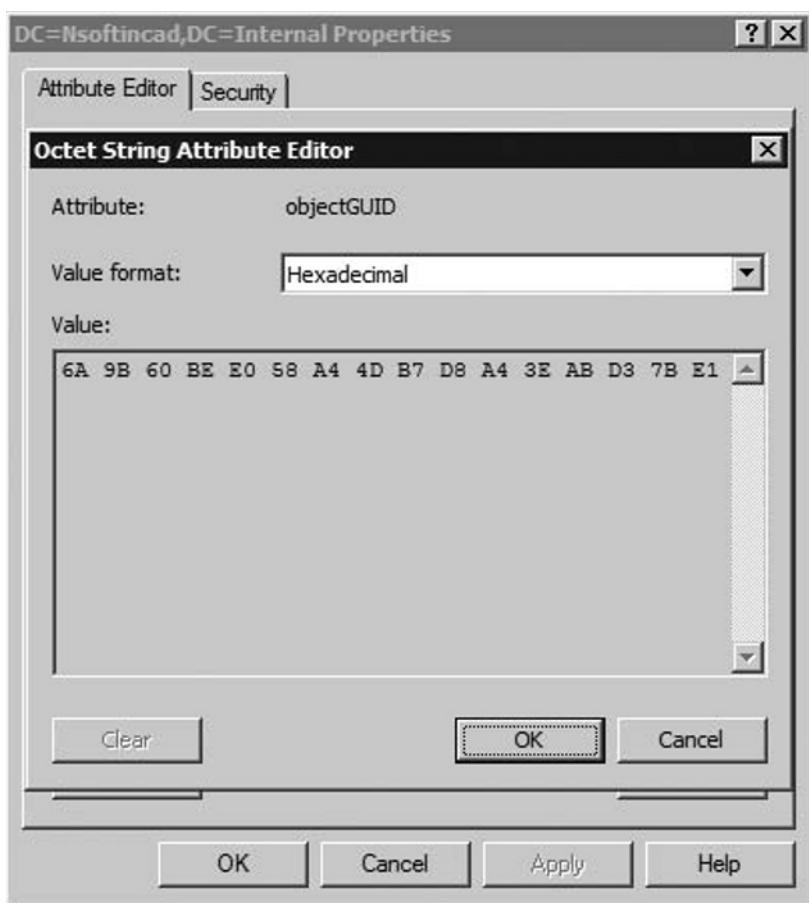
The structure starts with the character S identifying the object as a SID. Next is the revision level, which currently is always set to “1.” Then we have the identifier for the top-level authority that issued the SID—on our example this is “5” which means SECURITY_NT_AUTHORITY. The domain part is created during dcpromo and never changed. The RID is incremented during creation of a security principal, making the SID unique across the domain.

There are also “well-known” SIDs on a Windows system. These SIDs either always have the same structure, such as the SID for the Everyone Group (S-1-1-0), or have the same RID, such as the administrator account, which has always a RID of 544.

The Windows Security subsystem provides access to resources by evaluating SIDs. Why is this important in a restructuring scenario? Because we clone user accounts into the new forest—and cloning does not maintain the SID! During cloning, a new user account is created with a new SID. The new user account does not have access to resources in the source forest because of a SID mismatch between the old user account and the new user account.

The Object Global Unique Identifier in Active Directory

When you create an object in Active Directory, the system generates a unique identifier called the Global Unique Identifier (GUID) and assigns it to the object. The GUID is a 128-bit number that is unique in the forest and (theoretically) in the world. Compared to SIDs, GUIDs exist for *every* object in AD. During object deletion, GUIDs (like SIDs) are eliminated and not reused. In Figure 5.2, you will see the GUID of a domain object.

Figure 5.2 Domain Object GUID Revealed in ADSIEDIT

The Effect of an Upgrade or a Restructuring on SIDs and GUIDs

Upgrades and restructurings have different effects on existing SIDs and GUIDs. For example, in an upgrade scenario all SIDs are retained. A restructuring creates a new SID for every account that you migrate. GUIDs are retained in the same forest, but are created across forests. Table 5.1 shows when SIDs and GUIDs are retained and when they are created.

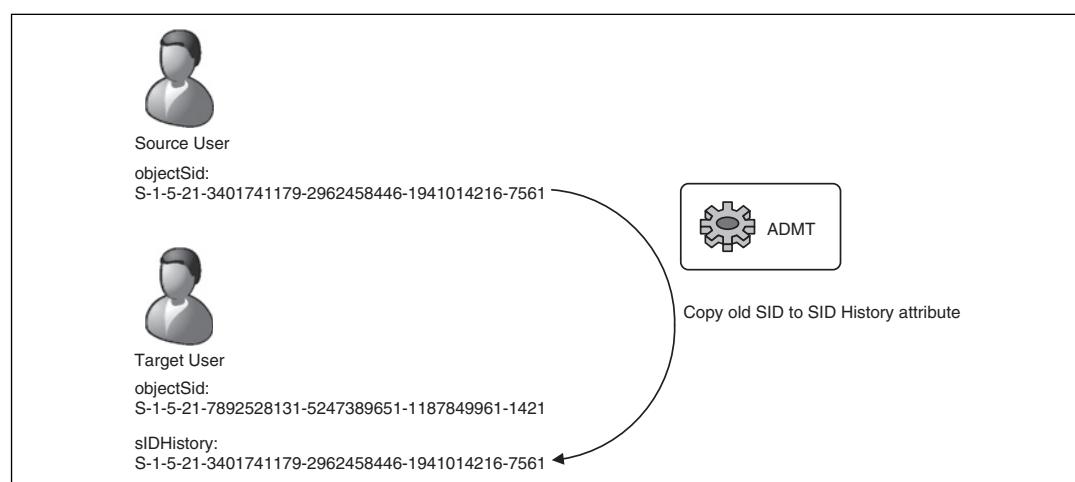
Table 5.1 Changes on SIDs and GUID during Upgrade and Restructuring

| Attribute | Effect during | | Inter-Forest restructuring |
|-----------|---------------|----------------------------|----------------------------|
| | Upgrade | Intra-Forest restructuring | |
| SID | SID retained | new SID created | new SID created |
| GUID | GUID retained | GUID retained | new GUID created |

Leveraging SID History to Maintain Access to Resources

SID History can help solve this problem. By using SID History, you maintain resource access without recreating access control lists on already-migrated systems in the target forest. SID History is an additional attribute on user and group objects in Active Directory. Your target domain(s) need to be at least in Windows 2000 Native Mode to use SID History.

So how does SID History work? During migration of a security principal, the SID of the old user account is copied into the SID History attribute of the new target account. Thus, the new target account has two SIDs and has access to both old and new systems and resources. To populate the SID History you use tools such as Active Directory Migration Tool (ADMT). Figure 5.3 shows how SID History migration works.

Figure 5.3 SID History Copying during User Migration

Using Active Directory Migration Tool to Restructure Domains

You can use Active Directory Migration Tool to restructure your environment. ADMT is a tool that allows you to migrate objects inside a forest or across forests. If necessary, it also can perform security translations on migrated objects to maintain resource access during the restructuring process. ADMT is available as a download from Microsoft: <http://go.microsoft.com/fwlink/?LinkId=75627>.

With ADMT, an administrator can migrate users, groups, service accounts, computers, and trusts, and perform security translation. ADMT is able to populate the SID History attribute and provides a password migration facility. ADMT tasks are performed from a console, a command line, or a script. You can automate the command line interface by using option files.

Before you use ADMT, make sure you configured DNS correctly and you have appropriate permissions in both forests. Name resolution must work in both directions to be able to create a trust relationship between the source and the target forest. For the migration to succeed, you need to be an administrator in both the source and the target forest.

NOTE

For Windows Server 2008 there will be a new version of ADMT. It is expected to be available in August 2008. Due to the lack of availability of the new version, we used ADMT Version 3 in our exercises. However, you must have at least one Windows Server 2003 Domain Controller installed in your Windows Server 2008 Domain, for ADMT V3 to run! If you have Windows Server 2008 domain controllers only, ADMT V3 will fail during migration.

The following exercises assume you have two forests configured: a source forest with a Windows Server 2003 domain controller and a Windows XP client computer, as well as a target forest with a Windows Server 2003 domain controller, which is the PDC Emulator role owner, and an additional Windows Server 2008 domain controller. In Exercise 5.1, you will install ADMT on a Windows Server 2003 domain controller in the target forest.

EXERCISE 5.1

INSTALLING ACTIVE DIRECTORY MIGRATION TOOL

1. Log on as a Domain Admin to a Windows Server 2003 domain controller in the target forest.
2. Click on **Start | Run**, type `<path>\admtsetup.exe`, and press **Enter**, where `<path>` is the path where the ADMT setup file is located.
3. On the **Welcome to the Active Directory Migration Tool Installation** page, click **Next**.
4. On the **License Agreement** page select **I agree** and click **Next**.
5. Wait until the Microsoft SQL Server Desktop Engine (MS_ADMT) is completed.
6. On the **Database Selection** page select **Use Microsoft SQL Server Desktop Edition (Windows)** and click **Next**.
7. Select **No, do not import data from an ADMT v2 database (Default)** on the **Active Directory Migration Tool v2 Database Import** page and click **Next**.
8. Click **Finish** to complete the installation.

Head of the Class...

SID Filtering

One security concern when using trusts is a malicious user who has administrative credentials in the trusted domain sniffing the trusting domain to obtain the credentials of an administrator account. With the credentials of the trusting domain administrator, the malicious user could add his SID to allow full access to the trusting domain's resources. This type of threat is called an elevation of privilege attack.

The security mechanism used by Windows Server 2003 and Windows Server 2008 to counter an elevation of privilege attack is SID filtering (as shown in Figure 5.4). SID filtering is used to verify that an authentication request coming in from the trusted domain only contains the domain SIDs

Continued

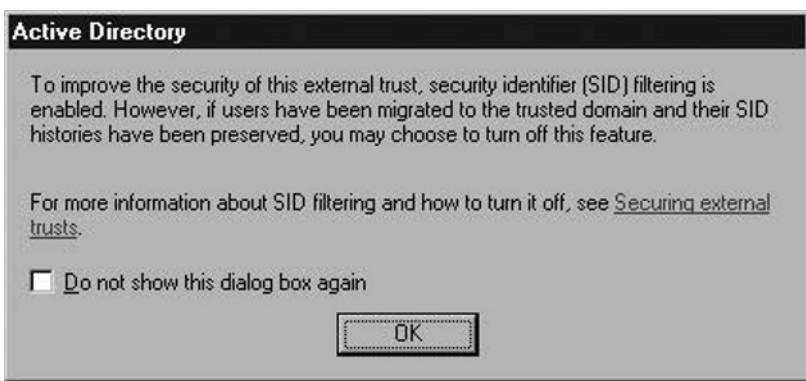
of the trusted domain. It does this by using the SIDHistory attribute on a security principal.

SID filtering uses the domain SID to verify each security principal. If a security principal includes a domain SID other than one from trusted domains, the SID filtering process removes the SID in question. This is done to protect the integrity of the trusting domain. This will prevent the malicious user from being able to elevate his or her privileges or those of other users.

There are some potential problems associated with SID filtering. It is possible for a user whose SID contains SID information from a domain that is not trusted to be denied access to the resources in the trusting domain. This can be a problem when universal groups are used. Universal groups should be verified to contain only users that belong to the trusted domain.

You can disable SID filtering if there is a high level of trust for all administrators in the affected domains. There are strict requirements to verify all universal group memberships, and any migrated users have their SIDHistories preserved. To disable SID filtering, use the **/EnableSIDHistory** option of the **netdom trust** command.

Figure 5.4 SID Filtering Warning When a Trust Is Created



EXERCISE 5.2

PREPARING THE PDC EMULATOR IN THE SOURCE DOMAIN

1. Log on as a Domain Admin to the PDC Emulator role holder in the source forest.
2. Click on **Start | Run**, in the open box type **REGEDIT**, and press **Enter**.

3. Navigate to the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

4. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
 5. Type **TcpipClientSupport** in the name field, and then press **Enter**.
 6. Double-click **TcpipClientSupport**.
 7. In **Value data**, type **1**, and then click **OK**.
 8. Close Registry Editor, and then restart the computer.
-

Maintaining User Passwords During a Restructure

From a user perspective, a restructuring should impact work at a minimum. One important factor is users' passwords. Telling users that they have to change their passwords can increase support costs because users tend to forget their new password or are not able to find a password that conforms to password policy rules. Some of the companies I worked with take a restructure as a chance to introduce new, stronger password policies. This requires a good communication plan, to prepare users for the upcoming change. Other companies don't take the challenge and maintain user passwords during a restructure.

If your choice is to maintain passwords, you need to take preparatory steps before you migrate passwords. Make sure the password policy defines requirements that are not stronger than the existing policy. Failure to do so will result in failed user account migrations. As a best practice you should also set the **Password never expires** option on all user accounts during the restructure process. Finally, to migrate passwords you need to use the ADMT "password export server" (PES) service, which must be installed at the source domain. The PES installation is a two-step process. First you create a key-file in the target domain that is bound to the source domain. Then you install the PES Service on the PDC Emulator FMSO role holder in the source domain by specifying the key-file.

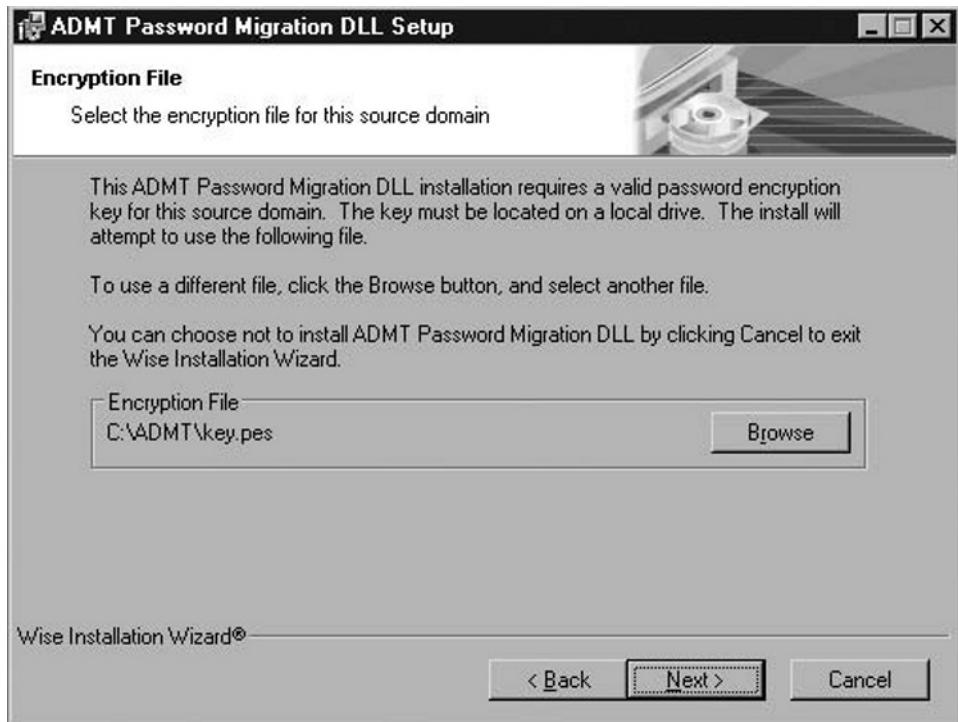
EXERCISE 5.3

INSTALLING PASSWORD EXPORT SERVER

1. Log on as a Domain Admin to a Domain Controller in the target forest.
2. Click on **Start | Run**, in the open box type **cmd**, and press **Enter**.
3. Type **net share PES=c:\Windows\ADMT\PES**. This will share the folder C:\Windows\ADMT\PES under the name PES.

4. Type **admt key /option:create /sourcedomain:<SourceDomainName> /keyfile: C:\Windows\ADMT\PES\key.pes**. This will create the encryption key-file for the source domain.
5. Log on as a Domain Admin to the PDC Emulator role holder in the source forest.
6. Click on **Start | Run**, in the open box type **\<Target Domain DC Name>\PES**, and press **Enter**. **<Target Domain DC Name>** is the name of the domain controller in the target domain where you created the key-file.
7. Copy the file **key.pes** to a local folder **c:\ADMT**, then double-click the **PwdMig.msi** file.
8. On the **Open File—Security Warning** box click **Run**.
9. On the **Welcome to the ADMT Password Migration DLL Installation Wizard** page click **Next**.
10. On the **Encryption File** page click **Browse** and then open the file **C:\ADMT\PES**. See Figure 5.5.

Figure 5.5 PES Encryption Key Selection



11. Click **Next** on the **Start Installation** page.
 12. On the **ADMT Password Migration DLL** box that appears, specify the **Domain Administrator of the target domain** as the service account name, enter the **password**, and click **Next**.
 13. Click **Finish** to complete the installation. Do not reboot the system.
 14. Click on **Start | All Programs | Administrative Tools | Services**.
 15. In the Services Console make sure that the startup type for the **Password Export Server Service** is set to **automatic**.
 16. Click **Start | Run**, in the open box type **REGEDIT**, and press **Enter**.
 17. Navigate to the following registry subkey:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA`
 18. Double-click **AllowPasswordExport**.
 19. In **Value data**, type **1**, and then click **OK**.
 20. Close Registry Editor, and then restart the computer.
-

Migrating Users and Groups

When you migrate users and groups, take into account that group membership must also be migrated. ADMT does this automatically for you, but it only works if you migrate objects in the correct order. If you migrate users first, copying of group membership information will fail, because of the way group membership information is stored in Active Directory. On a user object, AD stores group membership in the *memberof* attribute, members of a group are stored in the *members* attribute on a group. These attributes are back-linked, meaning that if you delete a value on one side (for example on the user side) the value is also deleted on the other side (the group). Back to our migration example: You migrate a user which is a member of several groups. None of the groups has been migrated so far. When ADMT creates the user object and then updates the *memberof* attribute it fails, because Active Directory does not know where to store the back-link.

To make a long story short, for a smooth migration you should migrate groups first and then migrate users. You configure ADMT to migrate group objects without populating the *members* attribute, then you migrate user objects and configure ADMT to update group membership on already migrated groups. Voila!

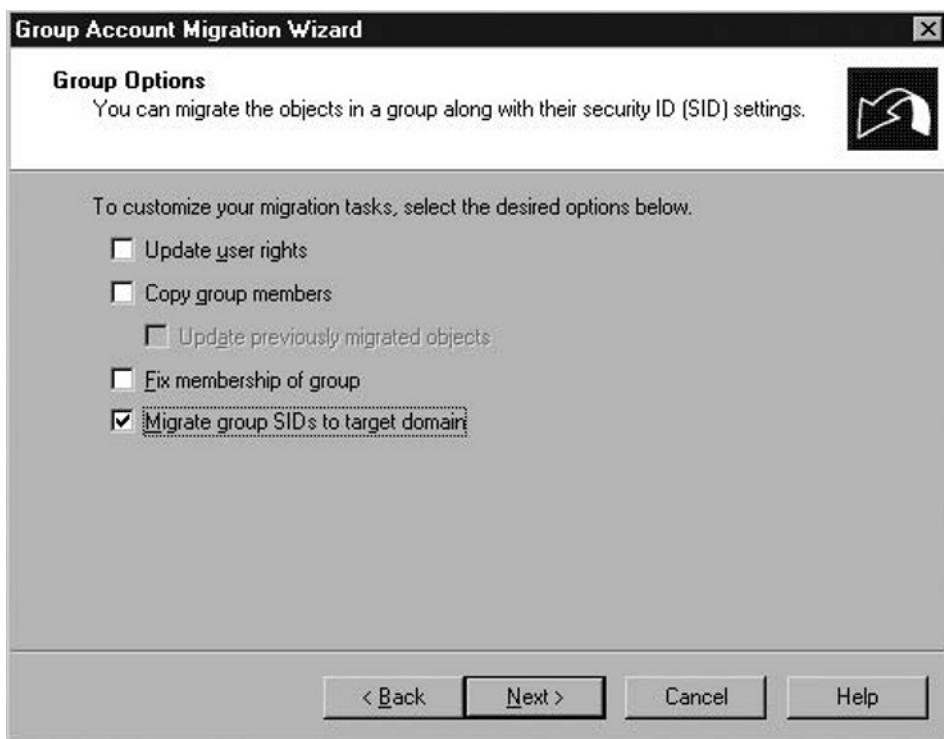
In the following exercises you will migrate group and user accounts and examine the SID History attribute on migrated objects.

EXERCISE 5.4

MIGRATING GROUP ACCOUNTS

1. Log on as a Domain Admin to a Windows Server 2003 domain controller in the target forest.
2. Click on Start | All Programs | Administrative Tools | Active Directory Migration Tool.
3. In the console tree right-click Active Directory Migration Tool and select Group Account Migration Wizard.
4. On the Welcome to the Group Account Migration Wizard page click Next.
5. On the Domain Selection page, select the source domain/source domain controller and target domain/target domain controller by using the drop-down boxes.
6. Click Select groups from domain on the Group Selection Option page and click Next.
7. On the Group Selection page, click add, type in the name of the group you want to migrate, click OK, and then click Next.
8. On the Organizational Unit Selection page click Browse, select the Users container of your target domain, and click Next.
9. Clear the Fix membership of group checkbox and select the Migrate group SIDs to target domain checkbox on the Group options page. See Figure 5.6.

Figure 5.6 Using SID History during Group Migration in ADMT



10. On the **Error** box click **Yes** to enable auditing in the source domain.
11. On the **Error** box click **Yes** to enable auditing in the target domain.
12. On the **Error** box click **Yes** to create the group **<SourceDomainName>\$\$\$** in the source domain.
13. On the **User account** page, type the **username** and the **password** of the administrator account of the source domain and click **Next**.
14. On the **Object Property Exclusion** page leave the defaults and click **Next**.
15. On the **Conflict Management** page leave the defaults and click **Next**.
16. Click **Finish** on the **Completing the Group Account Migration Wizard** page to start the migration.
17. Wait until the **Status** field in the **Migration Progress** window changes to **complete** and then click **Close**.



TEST DAY TIP

When we talked about SIDs, you learned that every Windows system consists of well-known SIDs such as the SID for built-in Groups or Users. These well-known SIDs cannot be migrated because their RID value is the same on both the source and the target system. Therefore, ADMT does not migrate built-in users or groups such as the *administrators* or *server operators* group. You are responsible to update group membership of those local groups after migration. This can be done either manually or in a scripted manner.

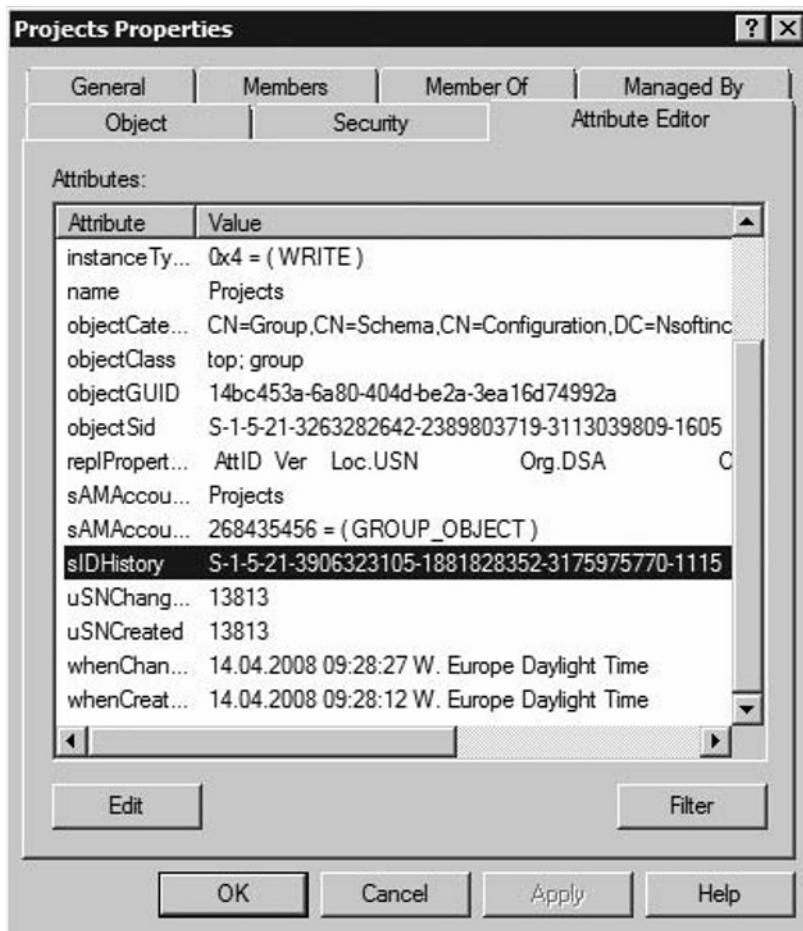
After you successfully migrated group accounts, you can check if the SID History attribute has been populated by using Active Directory Users and Computers on a Windows Server 2008 domain controller.

EXERCISE 5.5

EXAMINING THE SID HISTORY ATTRIBUTE

1. Log on as a Domain Admin to a Windows Server 2008 domain controller in the target forest.
2. Click on **Start | All Programs | Administrative Tools | Active Directory Users and Computers**.
3. On the **View** Menu, click **Advanced Features**.
4. In the console tree click on the **Users** container in the domain that you administering level.
5. In the right pane right-click the group that you previously migrated and select **Properties**.
6. In the **User Properties** dialog select the **Attribute Editor** tab.
7. Scroll down the list of attributes until you reach the **sIDHistory** attribute (See Figure 5.7).

Figure 5.7 Examining the SID History Attribute in Active Directory Users and Computers



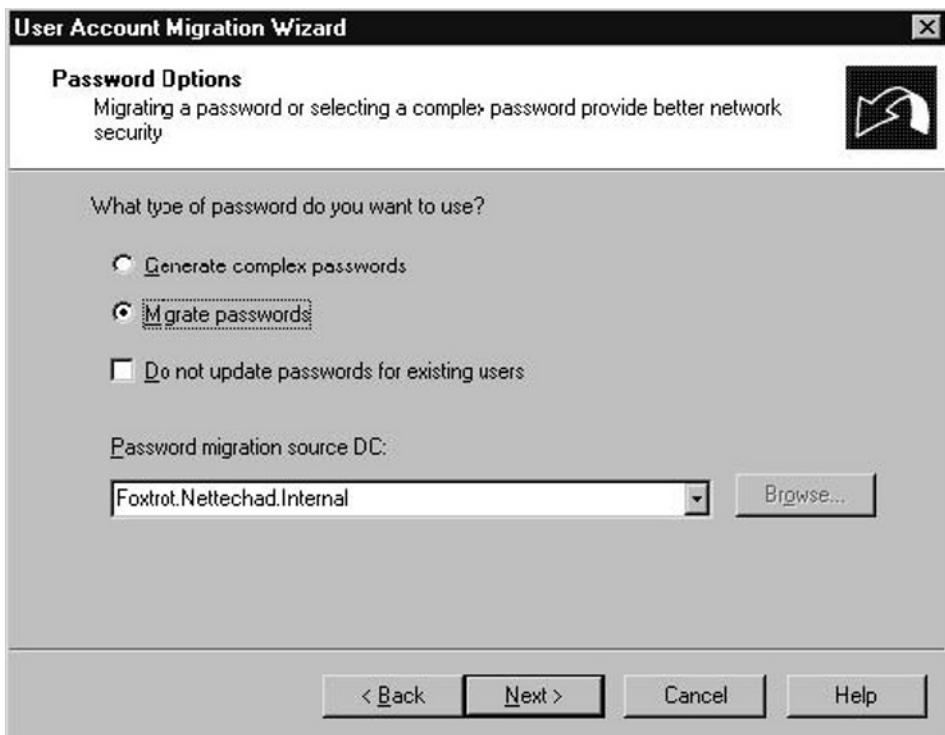
EXERCISE 5.6

MIGRATING USER ACCOUNTS

1. Log on as a Domain Admin to a Windows Server 2008 domain controller in the target forest.
2. Click on **Start | All Programs | Administrative Tools | Active Directory Migration Tool**.
3. In the console tree right-click **Active Directory Migration Tool** and select **User Account Migration Wizard**.

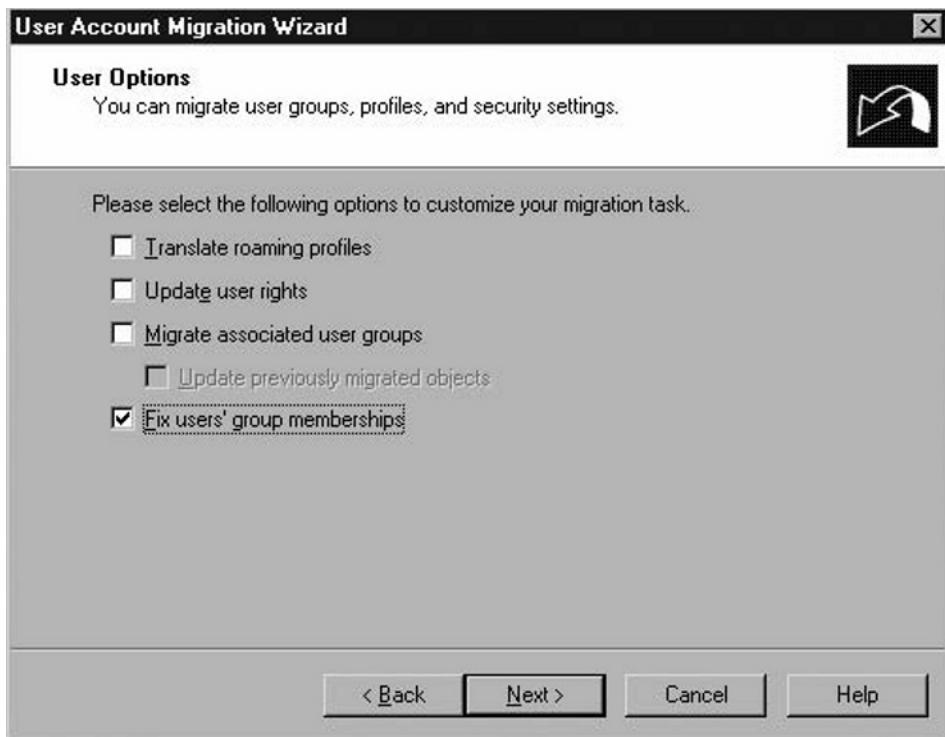
4. On the **Welcome to the User Account Migration Wizard** page click **Next**.
5. On the **Domain Selection** page, select the source domain/source domain controller and target domain/target domain controller by using the drop-down boxes.
6. Click **Select users from domain** on the **User Selection Option** page and click **Next**.
7. On the **User Selection** page, click **add**, type in the name of the user you want to migrate, click **OK**, and then click **Next**.
8. On the **Organizational Unit Selection** page click **Browse**, select the **Users** container of your target domain, and click **Next**.
9. On the **Password Options** page select **Migrate Passwords** and make sure the **PDC emulator** of the source domain is selected in the **Password migrations source DC** drop-down box. See Figure 5.8.

Figure 5.8 Selecting Password Migration for User Accounts in ADMT



10. On the **Account Transition Options** page make sure **Migrate user SIDs to target domain** is selected and click **Next**.
11. On the **User account** page type the **username** and the **password** of the administrator account of the source domain and click **Next**.
12. Select the **Fix users' group membership** checkbox on the **User Options** page and click **Next** (See Figure 5.9).

Figure 5.9 Selecting “Fix users' group membership” to Update Group Membership in Target Domain



13. On the **Object Property Exclusion** page leave the defaults and click **Next**.
14. On the **Conflict Management** page leave the defaults and click **Next**.
15. Click **Finish** on the **Completing the Group Account Migration Wizard** page to start the migration.
16. Wait until the **Status** field in the **Migration Progress** window changes to **Complete** and then click **Close**.

Migrating Computer Accounts

Computer Account migration uses an agent which will be installed automatically on client computers. The agent allows you to migrate local user profiles, local users, translate security on the file system and the registry, and of course changes the domain membership of the computer. It also includes reporting functionality.

In the following exercise you will migrate a computer account to a new domain.

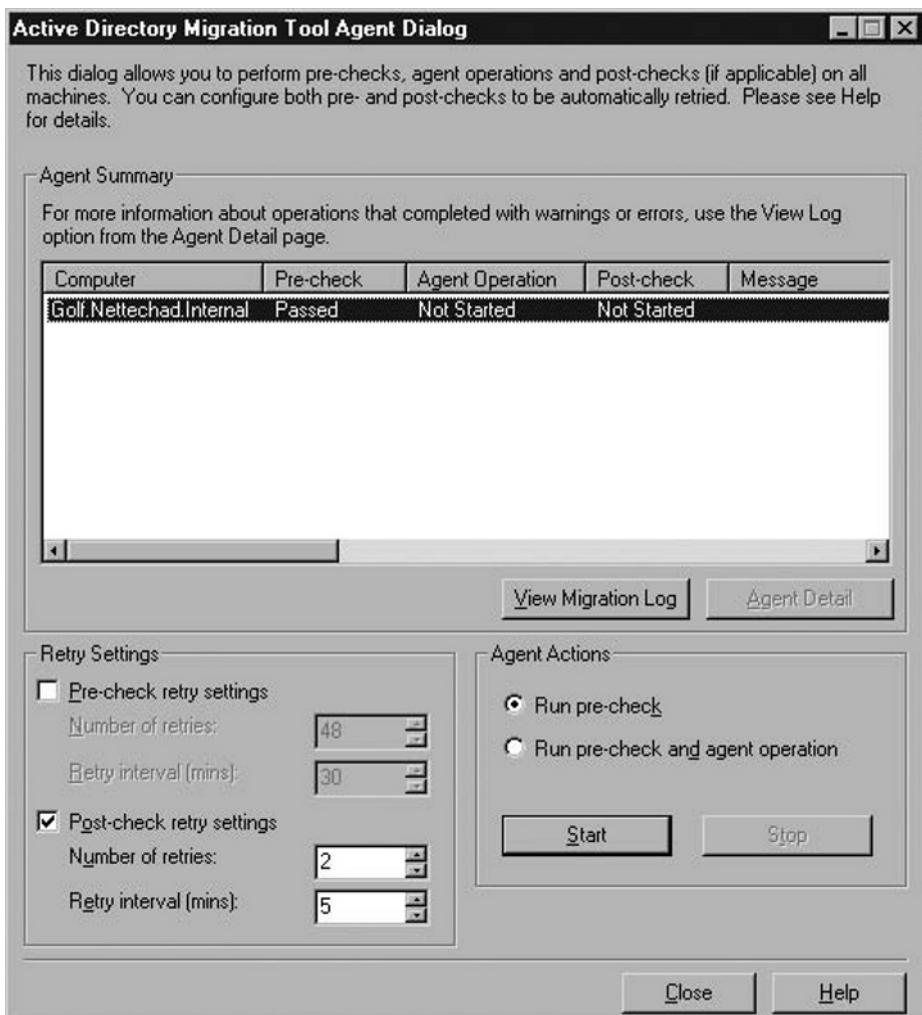
EXERCISE 5.7

MIGRATING A COMPUTER

1. Log on as the administrator of the source domain to a Windows Server 2003 domain controller in the target forest.
2. Click on **Start | All Programs | Administrative Tools | Active Directory Migration Tool**.
3. In the console tree right-click **Active Directory Migration Tool** and select **Computer Migration Wizard**.
4. On the **Welcome to the Computer Migration Wizard** page click **Next**.
5. On the **Domain Selection** page, select the source domain/source domain controller and target domain/target domain controller by using the drop-down boxes.
6. Click **Select computers from domain** on the **Computer Selection Option** page and click **Next**.
7. On the **Computer Selection** page, click **add**, type in the name of the computer you want to migrate, click **OK**, and then click **Next**.
8. On the **Organizational Unit Selection** page, click **Browse**, select the **Computers** container of your target domain, and click **Next**.
9. On the **Translate Objects** page select the checkboxes for the objects you want the security to be translated for and click **Next**.
10. Select **Add** on the **Security Translation options** page and click **Next**.
11. On the **Computer Options** page type **1** in the drop-down files and click **Next**.
12. On the **Object Property Exclusion** page leave the defaults and click **Next**.
13. On the **Conflict Management** page leave the defaults and click **Next**.

14. Click **Finish** on the **Completing the Computer Migration Wizard** page to start the migration.
15. Wait until the **Status** field in the **Migration Progress** window changes to **complete** and then click **Close**.
16. On the **Active Directory Migration Tool Agent** dialog select the line that represents your client computer from the list box.
17. On the **Active Directory Migration Tool Agent** dialog under **Agent Actions**, select **Run pre-check** and click **Start** (see Figure 5.10).

Figure 5.10 Running a Migration Pre-Check on a Client Computer



18. After the pre-check is complete, on the **Active Directory Migration Tool Agent** dialog under **Agent Actions**, select **Run pre-check and agent operation** and click **Start**.
 19. Wait for the migration to complete and click **Close**.
-

Upgrading Your Active Directory Domain or Forest

Upgrading your existing Active Directory domain or forest means either you in-place upgrade existing domain controllers to Windows Server 2008 or fresh install an additional domain controller, running Windows Server 2008, into the domain. Both methods lead to an interoperability mode in which you have to maintain both operating system versions. Table 5.2 gives you an overview of the possible in-place upgrade paths for Windows Server 2008. In either case you have to prepare the Active Directory before introducing a domain controller running Windows Server 2008.

Table 5.2 Windows Server 2008 In-place Upgrade Matrix

| Windows Server 2003 editions | Upgrade to Windows Server 2008 | | |
|--|--------------------------------|------------|------------|
| | Standard | Enterprise | Datacenter |
| Windows Server 2003 Standard Edition with Service Pack 1 (SP1) | Yes | Yes | No |
| Windows Server 2003 Standard Edition with Service Pack 2 (SP2) | | | |
| Windows Server 2003 R2 Standard Edition | | | |
| Windows Server 2003 Enterprise Edition with SP1 | | | |
| Windows Server 2003 Enterprise Edition with SP2 | No | Yes | No |
| Windows Server 2003 R2 Enterprise Edition | | | |
| Windows Server 2003 Datacenter Edition with SP1 | | | |
| Windows Server 2003 Datacenter Edition with SP2 | No | No | Yes |
| Windows Server 2003 R2 Datacenter Edition | | | |

For the following reasons, a domain upgrade might be appropriate:

- You do not want to change your existing Active Directory Topology. Therefore your existing Active Directory infrastructure is similar to the proposed infrastructure. An upgrade is the appropriate way, because it does not change the Active Directory topology.
- The risk should be minimized. A domain upgrade preserves all directory services, objects, and settings and is the migration path with the minimum risk.
- You want to leverage new operating system features at an early stage in the migration process. However, new Active Directory features might not be available, because all domain controllers need to be upgraded or replaced and the Domain Functionality Level needs to be raised.
- You have limited work resources for the migration. A domain upgrade requires the fewest hardware or personnel resources to complete.
- Applications are compatible with the new environment. Especially directory integrated applications, such as Microsoft Exchange Server should influence your decision. Compatibility has to be verified in a lab environment.
- You have a limited budget for the migration. The ability to buy additional hardware might be limited. If your existing domain controller hardware is capable of running Windows Server 2008, then it is not necessary to purchase additional hardware for an upgrade.
- You do not want to use additional tools for the update.

A domain upgrade may not be appropriate when:

- You want to leverage all of the new Active Directory features immediately. A domain upgrade is inappropriate in this situation, because to use new Active Directory features you need to wait until all domain controllers are running Windows Server 2008 and the domain functional level can be raised to Windows Server 2008.
- Applications and services are not ready for the new operating system. Therefore an upgrade would impact your production environment.
- You want to reduce administrative effort by reducing the number of domains or domain controllers. A domain upgrade might reduce the number of domain controllers. The number of domains will be the same. Therefore, a domain upgrade might not be appropriate.

A domain upgrade also involves upgrading other networks' services on which domain controllers and other computers in your environment rely on. These services include but are not limited to: Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), Certificate Services, Terminal Services Licensing, and others. When you upgrade your domain, you need to make sure that these services are available during the transition phase and that you migrate them to the new operating system at the right moment.

Installing Windows Server 2008

Domain Controllers into an Existing Forest

To install a Windows Server 2008 domain controller into an existing forest, the domain functionality level must be at least Windows 2000 Native. To prepare for the installation you need to extend the schema first. After schema extensions are replicated throughout the forest, you prepare each domain for the installation of Windows Server 2008 domain controllers. If you plan the use of Read-only Domain Controllers, you further have to prepare the domain for this kind of installation. In the following exercises you will prepare Active Directory for Windows Server 2008 domain controller installation. In the first exercise you will verify the domain functionality level.

EXERCISE 5.8

VERIFYING THE DOMAIN FUNCTIONAL LEVEL

1. Log on as a Domain Admin of the domain you are checking.
2. Click on **Start | All Programs | Administrative Tools | Active Directory Users and Computers**.
3. Locate the domain in the console tree that you are going to raise in functional level. Right-click the domain and select **Raise Domain Functional Level**.
4. In the **Raise Domain Functional Level** dialog box, the current domain functional level appears under **Current domain functional level**.
5. Make sure the domain functional level is at least **Windows 2000 Native**.

In the next exercise you will extend Active Directory schema with Windows Server 2008 specific objects and attributes and prepare the domain for the

installation of Windows Server 2008 domain controllers. You will need the Windows Server 2008 DVD for this task.

EXERCISE 5.9

PREPARING ACTIVE DIRECTORY FOR THE INSTALLATION OF WINDOWS SERVER 2008 DOMAIN CONTROLLERS

1. Log on as a Schema Admin on the Schema Master FSMO holder of the forest you are preparing.
2. Click on **Start | Run**, in the open box type **CMD** and press **Enter**.
3. Type **cd /d <driveletter>:\source\adprep**, where **<driveletter>** is the drive letter of your DVD drive.
4. Type **adprep /forestprep** and press **Enter**.
5. Press **C** and then press **Enter** to start the schema extension
6. You should see output similar to this:

```
Opened Connection to Delta
SSPI Bind succeeded
Current Schema Version is 31
Upgrading schema to version 44
Connecting to "Delta"
Logging in as current user using SSPI
Importing directory from file "C:\WINDOWS\system32\sch32.1df"
Loading entries.....
18 entries modified successfully.

...
```

7. After the schema extension is complete, log on as a Domain Admin on the Infrastructure Master FSMO holder in the domain that you are preparing.
8. Click on **Start | Run**, in the open box type **CMD**, and press **Enter**.
9. Type **cd /d <driveletter>:\source\adprep**, where **<driveletter>** is the drive letter of your DVD drive.
10. Type **adprep /domainprep** and press **Enter**.
11. A message will appear telling you that **Adprep successfully updated the domain-wide information**.

Migration Planning

Active Directory migration requires thoughtful planning and design and a well-thought-out deployment plan. We talked earlier about the different reasons and business needs that drive a migration. One common reason is to take advantage of new features and technologies. Another reason is the reduction of administrative overhead.

The complex task of migrating Active Directory, be it an upgrade or a restructure, is made easier by separating the job into distinct phases. Because we talk about Microsoft technologies, I will give you a very brief introduction of the Frameworks that Microsoft offers to make a migration as smooth as possible. Microsoft Solutions Framework (MSF) is an approach for management of an IT project. With MSF you would separate a migration project into the following phases:

- **Envisioning** In this phase, high-level project objectives are defined. The process of creating an Active Directory design begins in this phase.
- **Planning** In this phase, business requirements of the organization are gathered and analyzed. Business requirements will determine the conceptual design, the logical design, the physical design, and ultimately the functional specifications for the Active Directory design. A key deliverable from the planning phase is the Active Directory design plan, which is the primary input in developing a migration deployment plan.
- **Developing** In this phase, the features, components, and other elements described in the functional specification document are constructed. Necessary Active Directory and related network infrastructure is developed.
- **Stabilizing** In this phase, the Active Directory plan is tested to ensure that all business requirements of the organization are met. Active Directory is piloted typically to a small number of computers and users in the organization. Incidents that arise are addressed and documented. Modifications to the Active Directory design are made before the infrastructure is deployed throughout the organization.
- **Deploying/migration** In the deploying/migration phase, the final Active Directory infrastructure design is implemented. The final design includes all necessary modifications that have been discovered in the pilot phase.

During migration planning you will also:

- Assign object and roles. Keep track of users, groups, and other objects and their required permissions in the target location.
- Assign object locations, knowing where to place users, groups, computers, and other objects in the target location. This is highly dependent on an Organizational Unit plan.
- Develop a test plan. The test plan ensures that you are able to systematically test the migration to identify any shortcomings that would endanger the final deployment.
- Create a rollback plan. If for any reason your migration leads to extended downtime, the rollback plan allows you to get to a pre-migration state.
- Establish administrative procedures. During migration you have to ensure that administrative responsibilities are well defined. This also includes designing a plan for delegation administration.

Knowing When to Restructure

In the restructure scenario, you either restructure and consolidate domains in your existing forest—also called an *intra-forest migration*—or you install a new forest in parallel to your existing forest, called an *inter-forest migration*.

The advantage of this approach is flexibility. You only migrate objects and computers that you really need in the target domain/forest. All other objects are left behind, therefore you get a chance to start a “garbage collection and deletion” of your infrastructure. In an inter-forest migration it also gives you the ability to retry object migration. If something goes wrong during a migration you can analyze the failure, fix it, and repeat the migration.

The disadvantage of a forest restructuring is its complexity. During the migration phase you need to ensure that all users have access to their resources. Regardless of the migration state of the resource, if a file server is already migrated, a user in the source domain/forest might still need to access resources on this file server. This kind of resource access needs to be maintained in both directions! An often underestimated service is DNS. Name resolution needs to be maintained for both the source and the target forest. Table 5.3 lists the differences between an inter-forest and an intra-forest domain restructure.

Table 5.3 Comparison between Intra-forest and Inter-Forest Migrations

| Migration Consideration | Intra-forest Restructure | Inter-forest Restructure |
|-------------------------|---|---|
| Object preservation | During migration, objects are “moved” and no longer exist in the source location. | Objects are cloned. The original object remains in the source location. |
| SID history maintenance | SID history is required. | SID history is optional, but recommended. |
| User Password migration | Passwords are always retained. | Password migration is optional, but recommended. |
| Local profile migration | Local Profiles are migrated automatically, because the GUID of the user is preserved. | Tools such as ADMT are required to migrate local profiles. |

Intra-Forest Domain Restructure

Restructuring your existing forest allows for consolidation of domains and can reduce the administrative complexity and overhead. The intra-forest restructuring process moves accounts between domains compared to the cloning approach used in an inter-forest restructuring. Hence, you cannot retry an object migration and have to plan carefully. Computer Account migration is done using a wizard which connects remotely to each computer and changes domain membership. For an intra-forest restructuring all target domains must be operating at the Windows 2000 native or Windows Server 2003 functional level.

SID History is used to maintain resource access. No additional trusts need to be created, because all domains in a forest connect through transitive trusts. ADMT or a similar tool is needed for an intra-forest migration. An Intra-Forest restructuring further reduces or simplifies:

- Active Directory replication traffic
- User and Group administration
- Group Policy Implementation

An Intra-Forest restructuring might be appropriate when:

- You want to consolidate your infrastructure. By migrating objects to a target domain inside the forest, domains can be retired.
- You have enough work resources to complete the migration. Due to its complexity, a restructuring needs more work force compared to a domain upgrade.
- The project schedule allows for the additional time it takes to build additional domain controllers and perhaps install other services into the target domain.
- Your budget allows you to buy additional hardware. Your target domain will need more resources due to the higher user count. However, virtualization might be a viable alternative in contrast to new hardware. You could start with a (partly) virtualized target domain. After you complete the restructuring you could reuse hardware from the retired domains to build physical domain controllers in the target domain.
- A cleanup of old domain accounts and resources is desirable. Because you only migrate objects and resources you need into the target domain, you get a chance to do a cleanup.
- Use of additional tools for the migration is not an issue. Migrating objects and computers inside the forest is only possible with additional tools that are not part of the operating system.

An Intra-Forest restructuring may not be appropriate when you don't have the time to extend the target domain. Building new domain controllers and other services takes more time. Installing applications, such as Microsoft Exchange, will also add time it takes to prepare the new forest.

An inter-forest restructure might be performed for business changes such as mergers or acquisitions. When you migrate objects between forests as part of the restructuring process, both the source and target domain environments exist simultaneously. During the restructuring process, objects such as users and groups are copied to the source forest. This is also referred to as *cloning*. This enables you to roll back to the source environment during the migration, if necessary. Computer Account migration is done using a wizard which connects remotely to each computer and changes domain membership.

The target forest is built according to the proposed infrastructure. All target domains must be operating at the Windows 2000 native or Windows Server 2003

functional level. Ideally, all domain controllers are running Windows Server 2008, and the domain and forest functionality level are Windows Server 2008.

You establish trust relationships between the source domain(s) and the target forest. If your source forest is already running at Windows Server 2003 forest functionality level, a forest trust is a more feasible way. Forest Trusts are transitive and therefore lower administration overhead for managing trusts by requiring fewer trust relationships. To maintain resource access, you use a tool, such as ADMT, that can populate the SID History attribute. Inter-Forest migrations are often used when companies split or merge.

A domain/forest restructuring might be appropriate when:

- You want to leverage all Windows Server 2008 Active Directory features from the beginning. The new forest will only be built with domain controllers running Windows Server 2008. Therefore it is possible to immediately switch to Windows Server 2008 Domain and Forest functional level.
- The existing domain infrastructure does not meet the requirements for an upgrade.
- You want to consolidate your infrastructure. By migrating to a new forest, fewer domains can be built and administration overhead will be reduced.
- You have enough work resources to complete the migration. Due to its complexity, a restructuring needs more work force compared to a domain upgrade.
- The project schedule allows for the additional time it takes to build a new forest and perhaps install other services into the new forest.
- Your budget allows you to buy additional hardware. However, virtualization might be a viable alternative in contrast to new hardware. You could start with a (partly) virtualized target forest. After you complete the restructuring you could reuse hardware from the source forest to build physical domain controllers in the target forest.
- A cleanup of the old environment is desirable. Because you only migrate objects and resources you need in the new forest, you get a chance to do a cleanup.
- Use of additional tools for the migration is not an issue. Migrating objects and computers to the new forest is only possible with additional tools that are not part of the operating system.

A restructuring may not be appropriate when:

- You don't have the time to built a completely new infrastructure. Building a new forest takes more time due to the preparation of the new structure. Installing applications, such as Microsoft Exchange, will also add time it takes to prepare the new forest.
- Your existing infrastructure meets all business requirements. This might sound obvious, but is often overseen. Why should you build a new forest from scratch, when your existing forest design is appropriate? Doing so would only incur additional cost by providing no advantage.

Intra-Forest Upgrade and Restructure

There will be situations where a company wants to upgrade to Windows Server 2008 without restructuring to a new forest, but also wants to reduce the number of domains inside the existing forest. Of course, it is possible to combine the upgrade and restructure process. Whether you start with the upgrade and then restructure or vice versa depends on your business requirements. Your business requirements might be to introduce a new application that only runs in a Windows Server 2008 Domain and to reduce the administrative overhead. In this scenario, the first step would be to upgrade an existing domain to provide the requirements for the application and then restructure the forest to further reduce administrative overhead.

Windows Server 2008 support for multiple password policies might be another reason for restructuring. Active Directory on Windows Server 2003 and Windows 2000 Server only supports one password policy per domain. This led to increased administrative overhead if your business required multiple password policies, because you had to implement and maintain a multi-domain environment. With Windows Server 2008 you can consolidate those domains and provide multiple password policies in one domain, hence lowering administrative overhead.

Upgrade and restructure is the appropriate migration path when:

- The existing domain structure is similar to the proposed Active Directory domain structure. An initial domain upgrade will maintain the existing topology. Differences in the topology can be managed through a restructure after the domain upgrade is complete.
- You want to leverage Windows Server 2008 features very early. The domain upgrade allows you to quickly migrate the whole domain and then use the Windows Server 2008 Active Directory features. Moving security principals within the forest to the final target domain can be done at a later time as the schedule allows.

- Restructuring is an option for the future but is not feasible at the moment. An upgrade benefits the organization by providing new features and functionality. Restructure is possible at any time in the future.
- Your organization wants to leverage new features in Windows Server 2008 Active Directory, but does not have the work resources to restructure at the moment. Upgrading the domain first will use minimal resources and resources can be allocated as the restructure is implemented.
- Because of a shortage of time and work resources, the use of additional tools for the migration is not possible at the moment but will be in the future. At first a domain upgrade does not involve the use of tools such as ADMT. When the schedule and work resources allow, restructuring can begin.

An upgrade followed by a restructure may not be appropriate when:

- Rapid deployment of the restructured environment is a migration goal.
- Using the upgrade and restructure path can take a while to implement. First the domains must be upgraded and stabilized; after this is finished, you can commence restructuring the existing Active Directory environment. If one of the goals is to have the restructured environment done quickly, the restructure path should be used.
- The existing domain structure is not similar to the proposed Active Directory domain structure. If your forest structure does not meet the requirements, then you should restructure to a new forest.

Head of the Class...

What about Directory-Enabled Applications?

So far we only spoke about Active Directory services and resources such as file servers. But what about other applications like Microsoft Exchange Server or a third-party application like an Enterprise Resource Planning (ERP) system? When you design your restructuring strategy, make sure you include those applications and services into your design. Directory integrated applications need special considerations when you want to migrate to a new forest.

Cross-Forest Authentication

Large enterprises often tend to operate more than one Active Directory forest. The reasons for this can be manifold. Some multinational companies want distinct environments in different countries. Companies merged in the past and there were not enough resources to merge IT environments. Also, technical reasons exist. For instance, to be able to separate schema changes, it is a common practice to have directory-enabled applications in a separate forest. These separate forests are also called *Resource forests*, because they host a service which users in an *account forest* leverage.

A cross-forest authentication scenario always involves the creation and the management of trusts. Remember, there are several types of trust that you can use to implement cross-forest authentication

- **Forest Trusts** A forest trust can only be created between the root domains in two forests. Both forests must be Windows Server 2003 or Windows Server 2008 forests. These trusts can be one- or two-way trusts. They are considered transitive trusts because the child domains inside the forest can authenticate themselves across the forest to access resources in the other forest. From a management perspective, these trusts are the most effective, because you only have to create one trust to cover all domains in both forests.
- **External Trusts** You use an external trust when you need to create a trust between domains outside of your forest. These trusts can be one- or two-way trusts. They are always non-transitive in nature. This means you have created an explicit trust between the two domains, and domains outside this trust are not affected. You can create an external trust to access resources in a domain in a different forest that is not already covered by a forest trust. Because of the administrative overhead associated with the higher number of trusts required, you should use External Trusts only when you cannot create a Forest Trust. For instance, if you have to trust a forest which is operating at Windows Server 2003 forest functionality level with a forest that is operating at Windows 2000 native forest functionality level.
- **Shortcut Trusts** Shortcut trusts are transitive in nature and can be either one-way or two-way. These are explicit trusts that you create when the need exists to optimize (“shortcut”) the authentication process. Without shortcut trusts in place, authentication travels up and down the domain tree using the default parent and child trusts, or by using the tree-root trusts. In large, complex organizations that use multiple trees, this path can become a bottleneck when authenticating users. To optimize access, the

network administrator can create an explicit shortcut trust directly to the target domain. You use these trusts when user accounts in one domain need regular access to the resources in another domain. Shortcut trusts can be either one- or two-way.

If you implement a forest trust and want users to be able to log on to workstations in both forests, consider implementing cross-forest Group Policy processing. GPO processing across forests is disabled by default but you can enable it via Group Policy. The same limitation also applies to roaming user profiles. If you enable GPO processing across forests, roaming user profiles will also be loaded across forests.

Implementation Planning

During your implementation planning you will take into account several factors that may affect your deployment. On closer examination, many of the factors that you should consider are typically part of a project management approach:

- Time constraints and resource availability will influence the decision about a quick or a lengthy migration.
- The tolerance for downtime of your organization affects your pilot testing and consequently your deployment.
- You will perform a Gap Analysis to be able to compare your current environment to the envisioned environment.
- Server placement planning will influence your server capacity planning, and furthermore, your budget planning.
- As long as you must support applications that are not fully compatible with your new environment, you cannot complete your migration.
- You should measure your organization's risk tolerance. Risk tolerance is your organization's tolerance to unexpected or unforeseen events. For example, does your organization accept risk to the production environment in relation to achieving a migration goal, such as speed or budget?

Planning for Interoperability

Business to Business (B2B) scenarios as well as business to customer (B2C) scenarios are typical cases where organizations extend the reach of their applications and services to reduce cost and complexity. A typical B2B scenario is that of a manufacturer and its supplier. The manufacturer orders goods from the supplier over the Internet.

To get access to the supplier Web site, the purchaser will need credentials to authenticate and to get authorized. Traditionally these credentials are maintained at the supplier site. The disadvantage of such a scenario is that the purchaser has to maintain an additional set of credentials, the supplier needs to maintain an additional set of credentials, and they also need to check the authorization for these credentials. Of course it would be possible to create trust relationships between those organizations, but this also requires a secure tunnel between them and in the end adds complexity and administrative overhead. Moreover, not all organizations operate on a Windows infrastructure.

Interorganizational Strategies

To reduce complexity and administrative overhead, organizations that do not operate on a Windows infrastructure could use the Web Services Architecture to build a trust relationship between their infrastructures. Built for platform interoperability, Web Services (WS) extend the functionality of the HTTP protocol. Most Web Services uses XML to transmit messages through HTTP. The format of such XML messages is defined in the Simple Object Access Protocol (SOAP) specification. To give users a reference on how to use a certain set of SOAP messages from an application, a Web Services Description File (WSDL) may be created. Think of it as an interface description file. Web Services are registered so that other companies or users can find them. This is done with Universal Description Discovery and Integration (UDDI). A UDDI entry is an XML file describing a business and the services it offers.

Web Services specifications define protocols that offer security, reliable messaging, and transactions in a Web Service environment. WS specifications include the WS-Security protocol which describes message integrity, message confidentiality, and single message authentication. WS-Security also provides an extensible interface for associating security tokens in SOAP messages.

Based on WS-Security, the WS-Trust protocol defines extensions to manage trusts and to issue and request security tokens. Finally, WS-Federation defines mechanisms that are used to federate across different trust realms and therefore enable the exchange of identity, attribute, authentication, and authorization information.

Active Directory Federation Services

Active Directory Federation Services (ADFS): You can use Active Directory Federation Services (ADFS) to create a highly extensible, Internet-scalable, and secure identity access solution that can operate across multiple platforms, including

both Windows and non-Windows environments. Essentially, this allows cross-forest authentication to external resources—such as another company’s Active Directory.

Federation Services were originally introduced in Windows Server 2003 R2. Federation provides an identity access solution, and AD Federation Services provides authenticated access to users inside (and outside) an organization to publicly (via the Internet) accessible applications. Federation Services provides an identity management solution that interoperates with WS-* Web Services Architecture–enabled security products. WS-Federation Passive Requestor Profile (WS-F PRP) also makes it possible for federation to work with solutions that do not use the Microsoft standard of identity management. The WS-Federation specification defines an integrated model for federating identity, authentication, and authorization across different trust realms and protocols. This specification defines how the WS-Federation model is applied to passive requestors such as Web browsers that support the HTTP protocol. WS-Federation Passive Requestor Profile was created in conjunction with some pretty large companies, including IBM, BEA Systems, Microsoft, VeriSign, and RSA Security.

What Is Federation?

As we described earlier in this chapter, federation is a technology solution that makes it possible for two entities to collaborate in a variety of ways. When servers are deployed in multiple organizations for federation, it is possible for corporations to share resources and account management in a trusted manner. This is just one way companies can take advantage of FS. With ADFS, partners can include external third parties, other departments, or subsidiaries in the same organization.

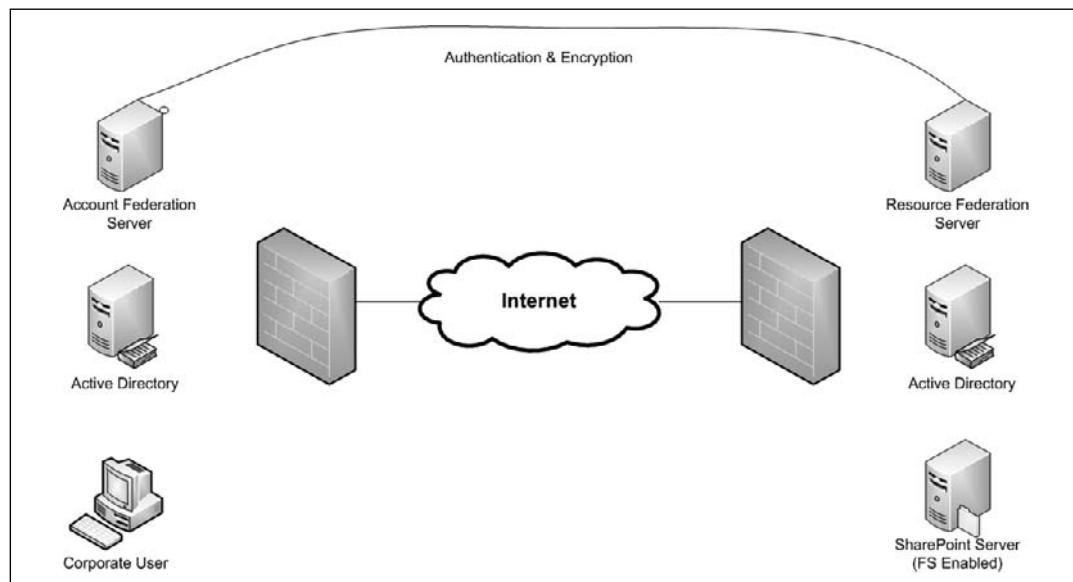
Why and When to Use Federation

Federation can be used in multiple ways. One product that has been using federation for quite some time is Microsoft Office Communication Server (previously, Live Communication Server 2005, now rebranded as Office Communication Server 2007). Federation is slightly different in this model, where two companies can federate their environments for the purposes of sharing presence information. This makes it possible for two companies to securely communicate via IM, Live Meeting, voice, and video. It also makes it possible to add “presence awareness” to many applications, including the Office suite, as well as Office SharePoint Server. If you want to know more about OCS and how federation works for presence, we recommend *How to Cheat at Administering Office Communications Server 2007*, also by Elsevier.

A little closer to home, Federation Services can also be used in a variety of ways. Let's take another B2B example where a company in the financial service business shares information with its partners. The company hosts a Windows SharePoint Services (WSS) site in their DMZ for the purposes of sharing revenue information with investment companies that sell their products. Prior to Active Directory Federation Services, these partners would be required to use a customer ID and password in order to access this data. For years, technology companies have been touting the ability to provide and use single sign-on (SSO) solutions. These worked great inside an organization, where you may have several different systems (Active Directory, IBM Tivoli, and Solaris), but tend to fail once you get outside the enterprise walls.

With ADFS, this company can federate their DMZ domain (or, their internal AD) with their partner Active Directory infrastructures. Now, rather than creating a username and password for employees at these partners, they can simply add the users (or groups) to the appropriate security groups in their own Active Directory (see Figure 5.11). It is also important to note that ADFS requires either Windows Server 2008 Enterprise edition or Datacenter edition.

Figure 5.11 The Active Directory Federation Services Structure



Prerequisites for ADFS

There are some prerequisites needed before you install ADFS. You probably guessed from the name that an Active Directory Service is needed. The good news is that ADFS in Windows Server 2008 can either use Active Directory Domain Services (ADDS) or Active Directory Lightweight Directory Services (ADLDS).

To issue certificates to your Web sites and for signing purposes you will need a Certification Authority such as Active Directory Certificate Services. However, in our exercise we will use self-signed certificates.

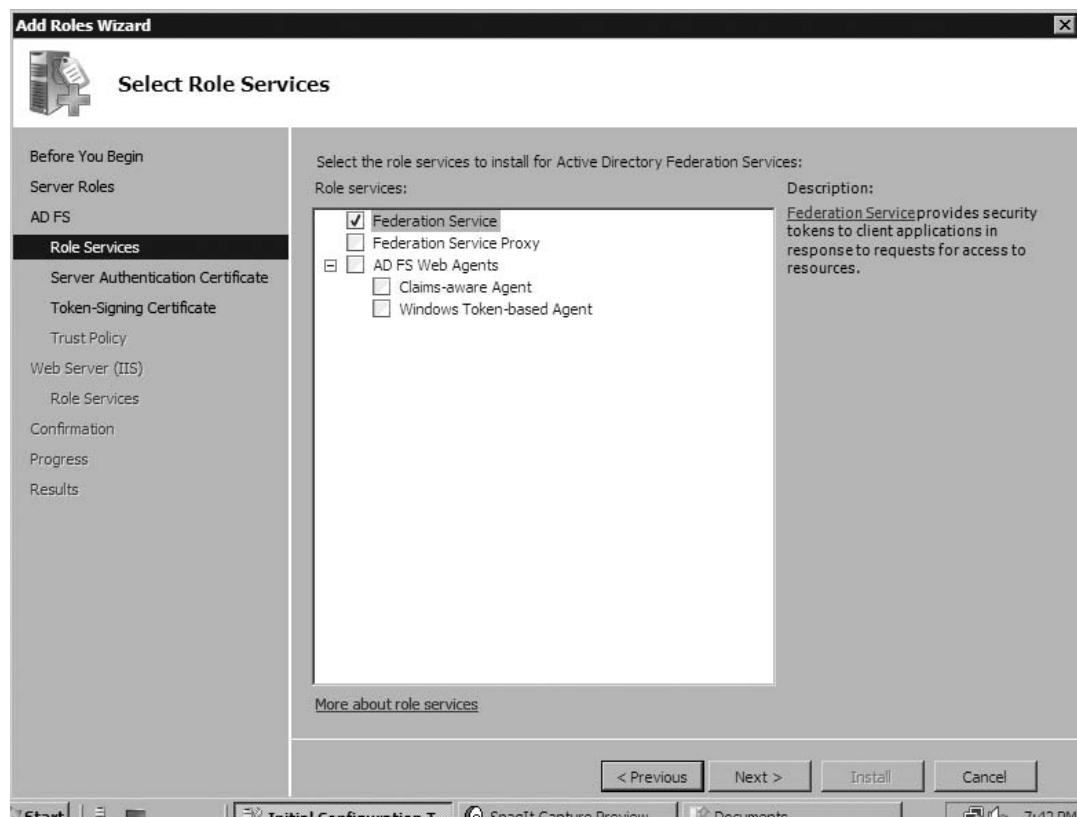
Configuring ADFS

In this exercise, we are going to create the account side of the ADFS structure. The resource is the other half of the ADFS configuration, which is the provider of the service that will be provided to an account domain. To put it in real-world terms, the resource would provide the extranet application to the partner company (the account domain).

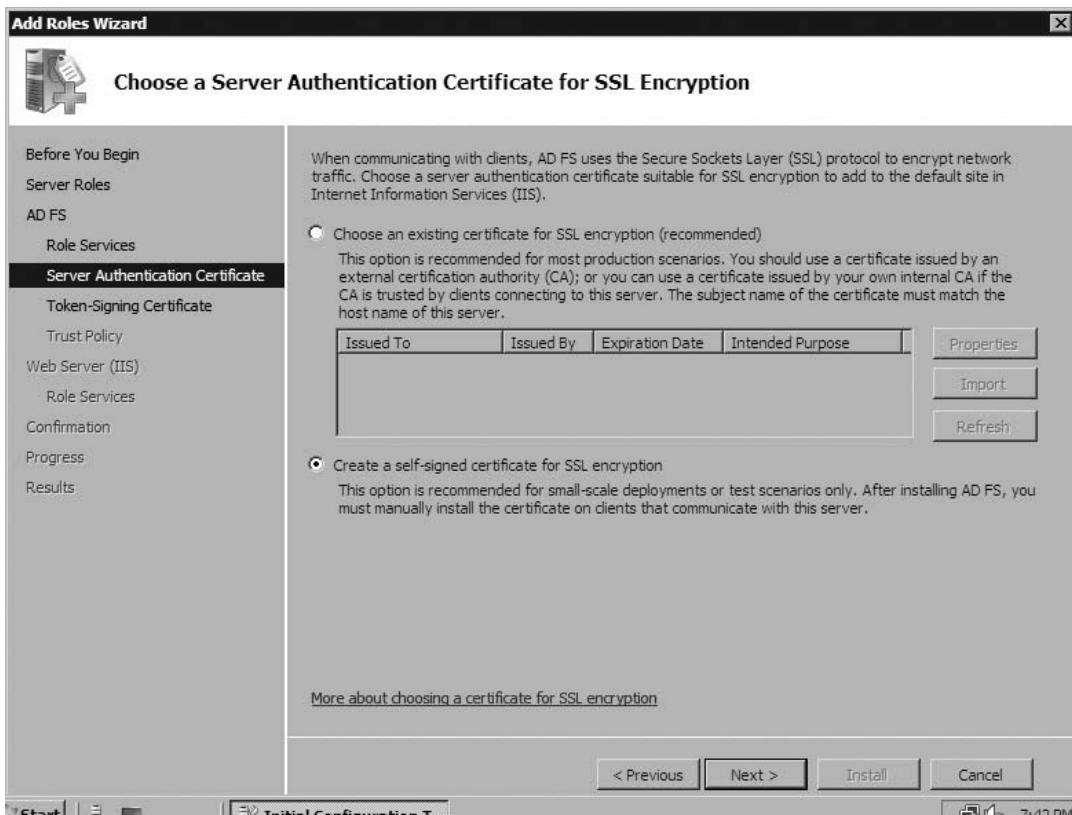
EXERCISE 5.10

CONFIGURING FEDERATION SERVICES

1. Click **Start | Administrative Tools | Server Manager**.
2. Scroll down to **Role Summary**, and then click **Add Roles**.
3. When the **Before You Begin** page opens, click **Next**.
4. On the **Select Server Roles** page, select **Active Directory Federation Services** (see Figure 5.12) from the list and click **Next**.

Figure 5.12 Selecting the Role

5. Click **Next** on the **Active Directory Federation Services** page.
6. In the **Select Role Services** window, select **Federation Service**, and then click **Next**. If prompted, add the additional prerequisite applications.
7. Click **Create A Self-Signed Certificate For SSL Encryption** (Figure 5.13), and then click **Next**.

Figure 5.13 Creating a Self-Signed Token-Signing Certificate

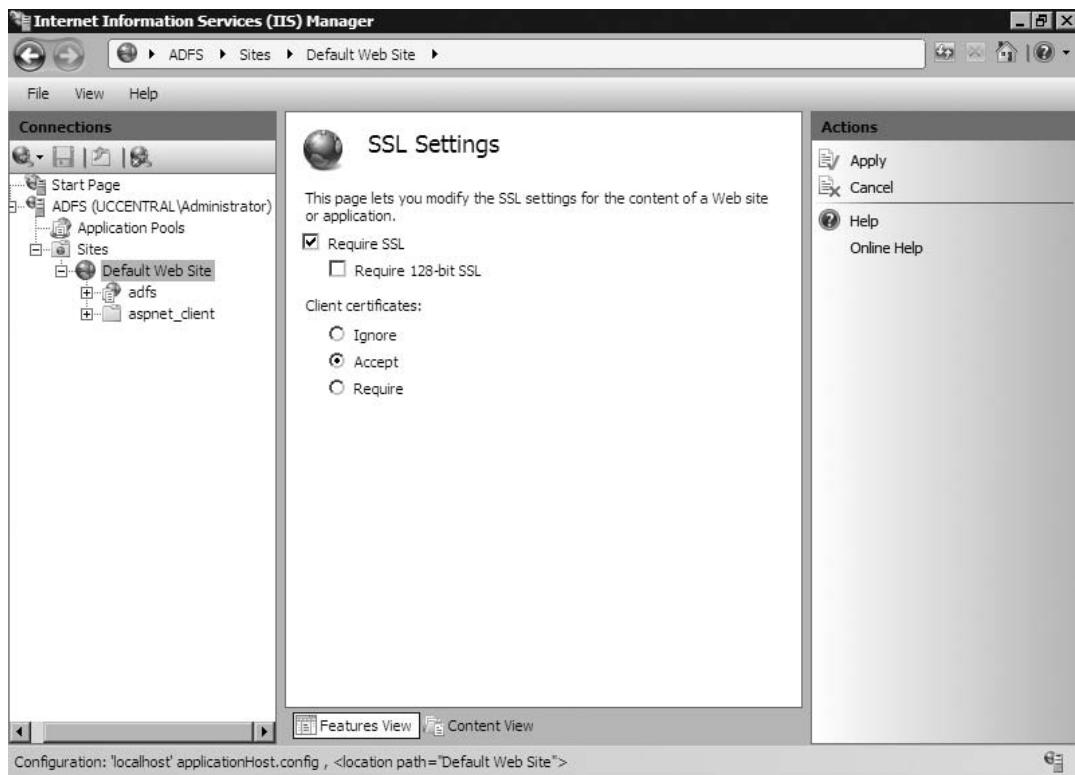
8. Click **Create A Self-Signed Token-Signing Certificate**, and then click **Next**.
9. Click **Next** on the **Select Trust Policy** page.
10. If prompted, click **Next** on the **Web Server (IIS)** page.
11. If prompted, click **Next** on the **Select Role Services** page.
12. On the **Confirm Installation Selections** page, click **Install**.
13. When the installation is complete, click **Close**.

The next step in configuring ADFS is to configure IIS to require SSL certificates on the Federation server:

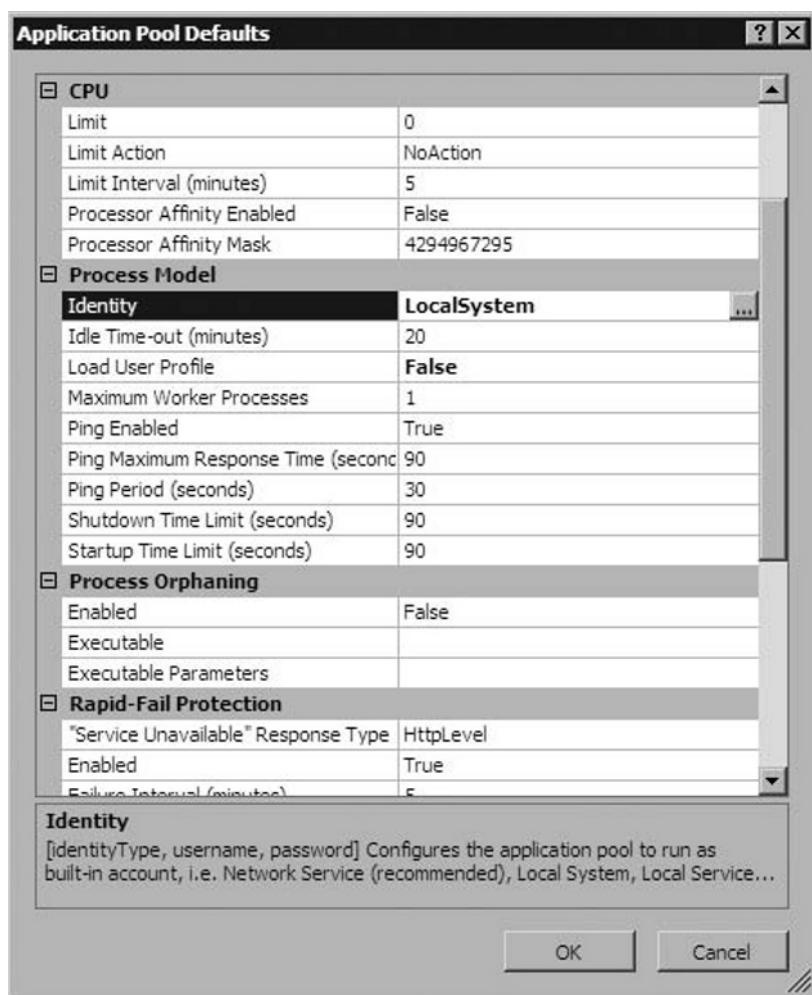
1. Choose **Start | Administrative Tools | Internet Information Services (IIS) Manager**.
2. Double-click the server name.
3. Drill down the left pane to the Default Web Site and double-click it.

4. Double-click **SSL Settings** and select **Require SSL**.
5. Go to **Client Certificates** and click **Accept**. Then, click **Apply** (Figure 5.14).

Figure 5.14 Requiring Client Certificates



6. Click **Application Pools**.
7. Right-click **ADFS AppPool**, and click **Set Application Pool Defaults**.
8. In the **Identity** pane (Figure 5.15), click **LocalSystem**, and then click **OK**.

Figure 5.15 Setting Application Pool Defaults

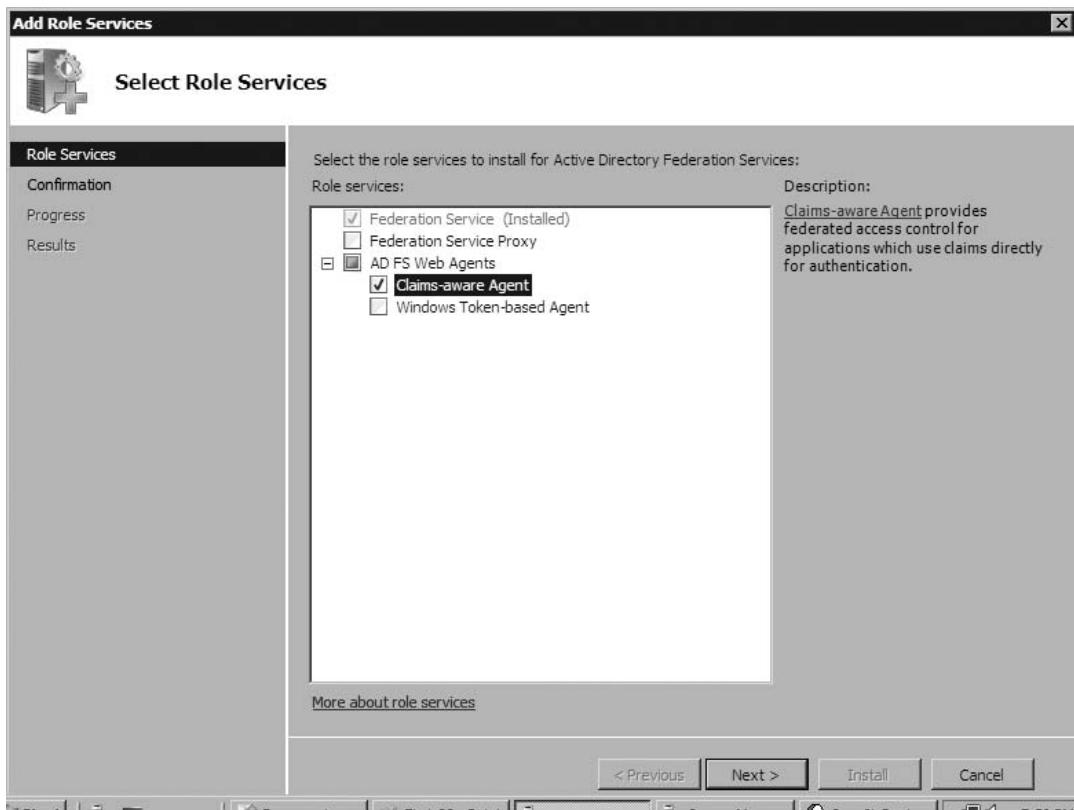
9. Click **OK** again.
10. Before we close IIS, we need to create a self-signed certificate. Double-click the server name again.
11. Double-click **Server Certificates**.
12. Click **Create Self-Signed Certificate**.
13. In the **Specify Friendly Name** field, enter the NetBIOS name of the server and click **OK**.

Next, we need to configure a resource for use with ADFS. In this case, we are going to use the same domain controller to double as a Web server.

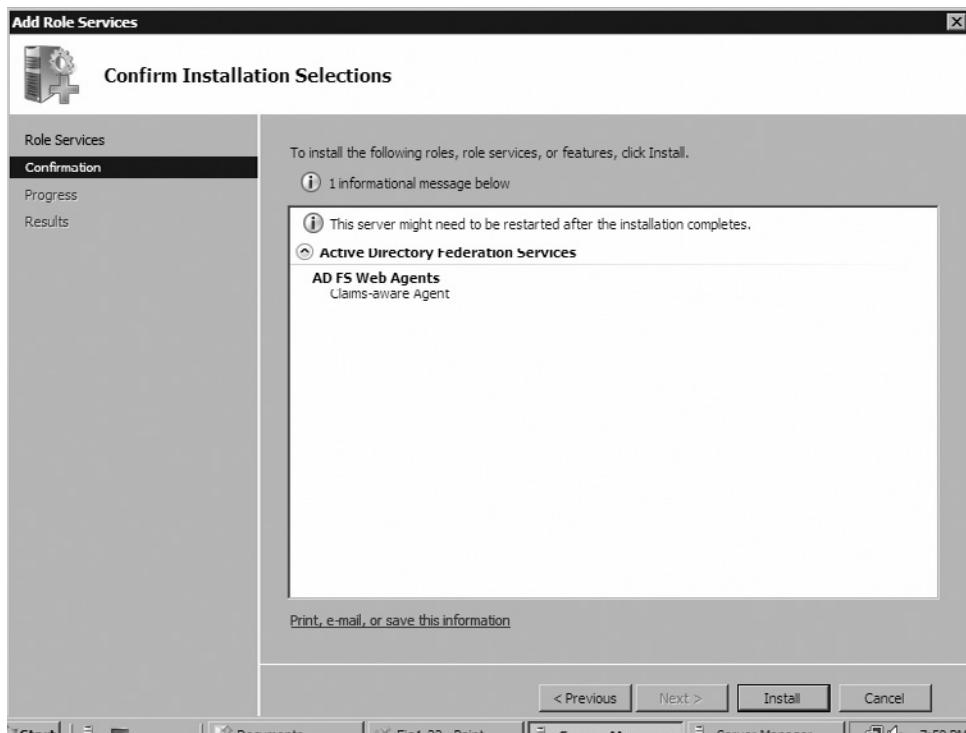
What we will be doing is installing the ADFS Web Agent, essentially adding an additional role to the server, as part of the ADFS architecture. This will allow us to use our federated services within a Web application.

1. Choose **Start | Administrative Tools | Server Manager**. Scroll down to **Role Summary**, and then click **Add Roles**.
2. When the **Before You Begin** page opens, click **Active Directory Federation Services**.
3. Scroll down to **Role Services** and click **Add Role Services**.
4. In the **Select Role Services** window, select **Claims-aware Agent** (Figure 5.16), and then click **Next**.

Figure 5.16 Setting Services



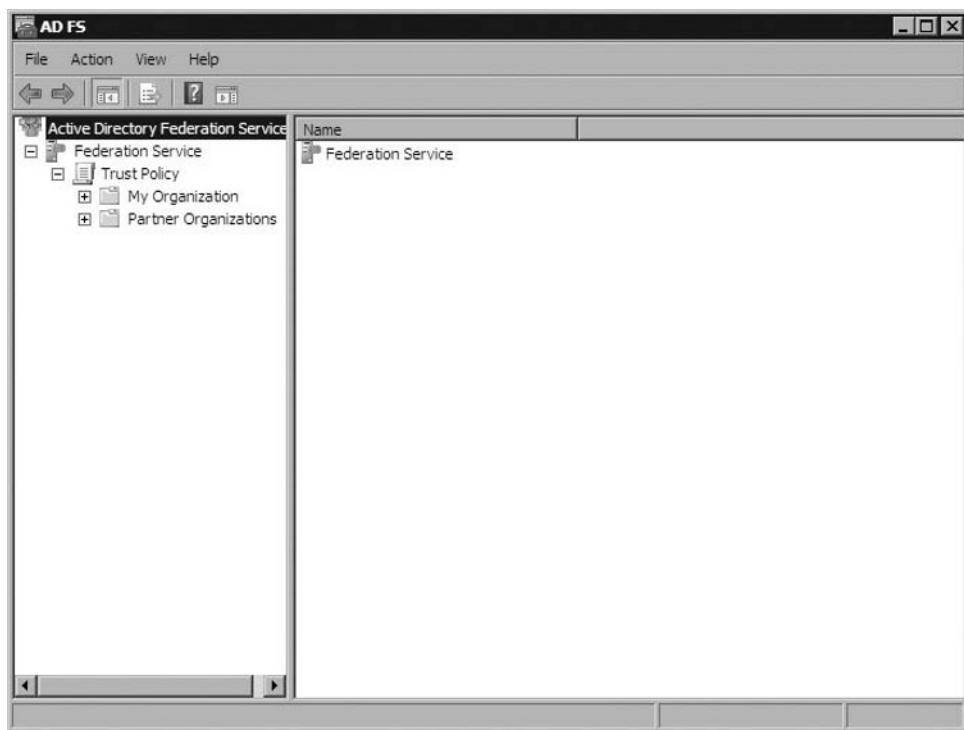
5. Confirm the installation selections (Figure 5.17), and then click **Install**.

Figure 5.17 Confirming the Installation

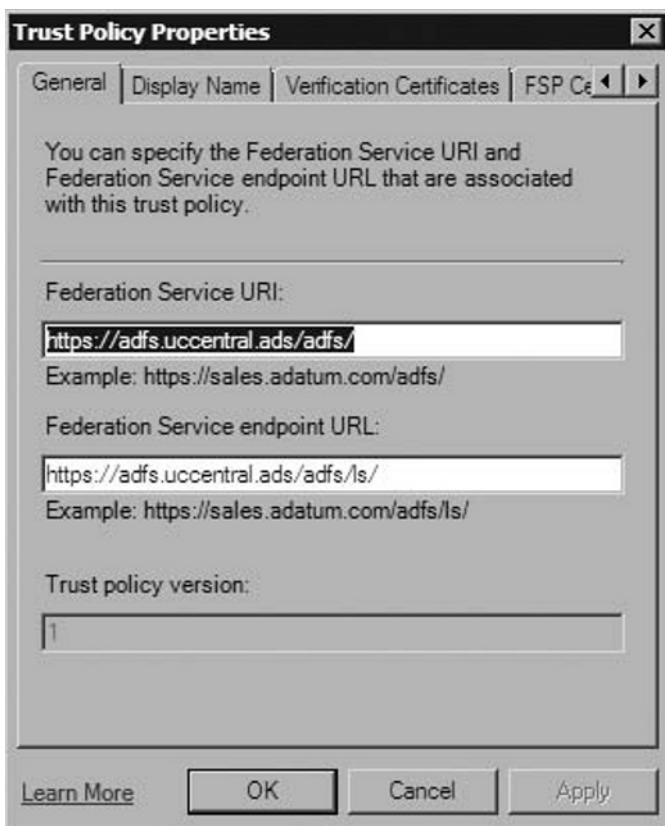
6. When installation is complete, click **Close**.

Now we need to configure the trust policy which would be responsible for federation with the resource domain.

1. Choose **Start | Administrative Tools | Active Directory Federation Services**.
2. Expand **Federation Service** by clicking the + symbol (see Figure 5.18).

Figure 5.18 ADFS MMC

3. Right-click **Trust Policy**, and then choose **Properties**.
4. Verify the information in Figure 5.19 matches your configuration (with the exception of the FQDN server name), and then click **OK**.

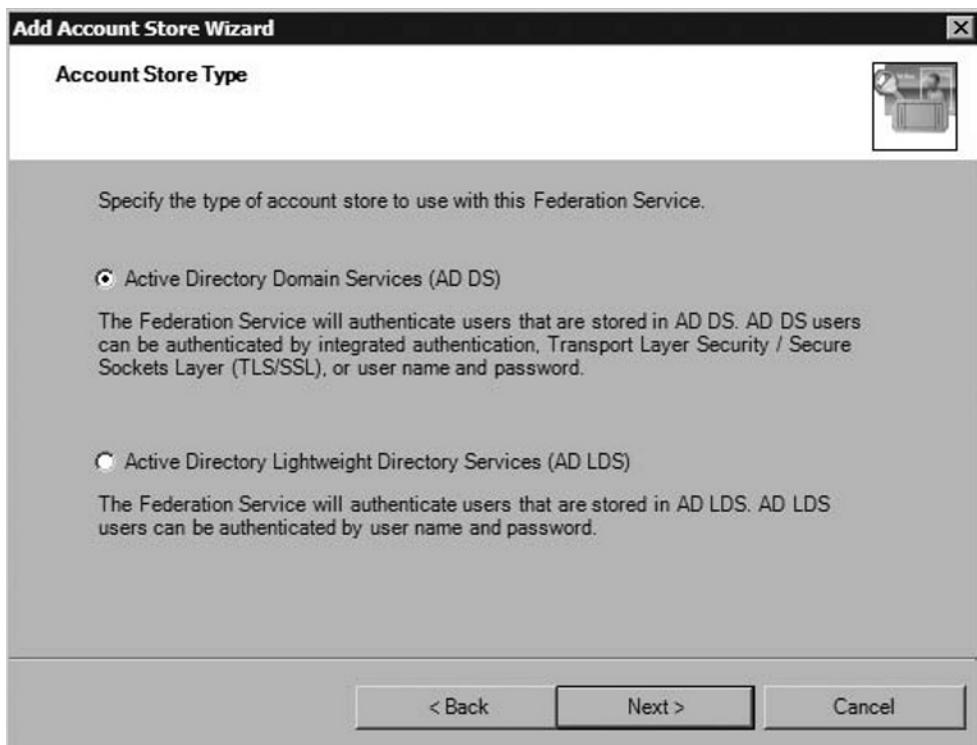
Figure 5.19 Trust Policies

5. When you return to the AD FS MMC, expand **Trust Policy** and open **My Organization**.
6. Right-click **Organization Claims**, and then click **New | Organization Claim**.
7. This is where you enter the information about the resource domain. A claim is a statement made by both partners and is used for authentication within applications. We will be using a **Group Claim**, which indicates membership in a group or role. Groups would generally follow business groups, such as accounting and IT.
8. Enter a claim name (we will use **PrepGuide Claim**). Verify that **Group Claim** is checked as well before clicking **OK**.
9. Create a new account store. Account stores are used by ADFS to log on users and extract claims for those users. ADFS supports two types of account stores: Active Directory Domain Services (ADDS) and Active Directory Lightweight Directory Services (AD LDS).

This makes it possible to provide ADFS for full Active Directory Domains and AD LDS domains.

10. Right-click **Account Store** and choose **New | Account Store**.
11. When the **Welcome** window opens, click **Next**.
12. Since we have a full ADDS in place, select **Active Directory Domain Services (AD DS)** from the **Account Store Type** window (Figure 5.20), and then click **Next**.

Figure 5.20 The Account Store Type Window

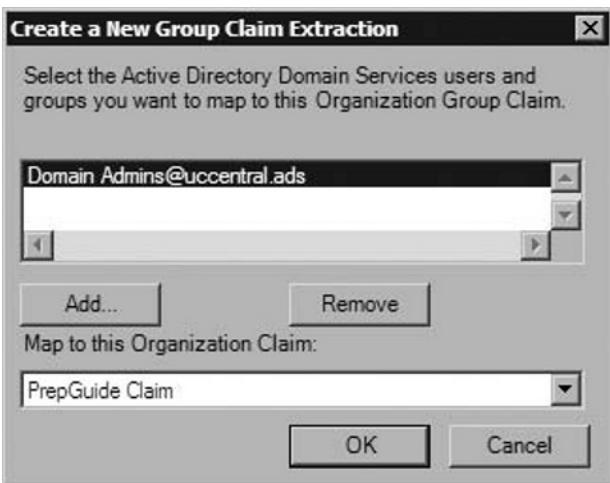


13. Click **Next** on the **Enable This Account Store** window.

14. Click **Finish** on the completion page.

Now, we need to add Active Directory groups into the Account Store.

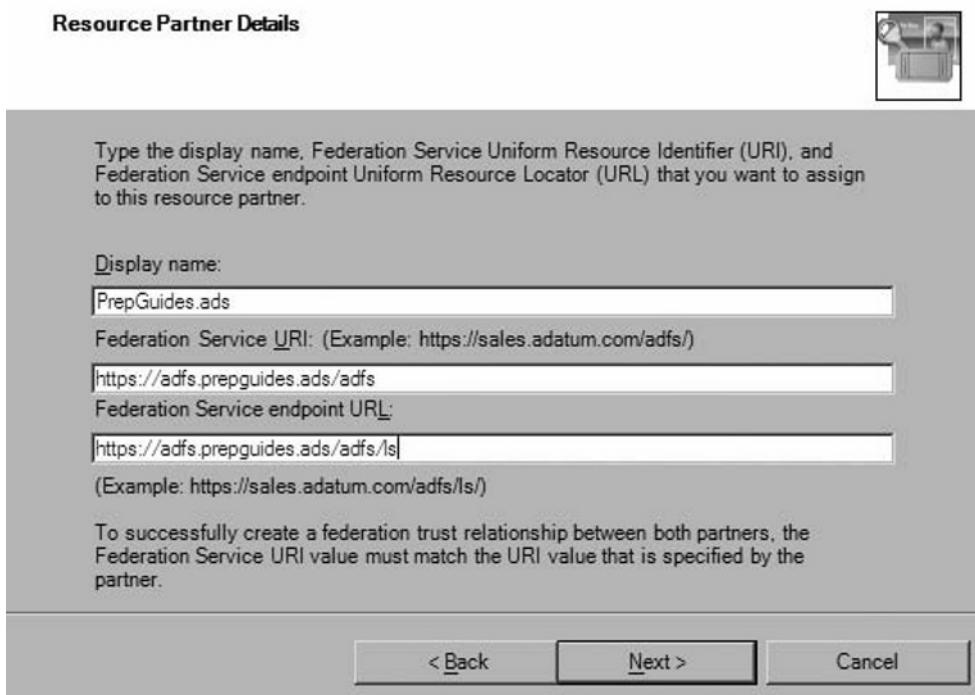
1. Expand **Account Stores**.
2. Right-click **Active Directory**, and then click **New | Group Claim Extraction**.
3. In the **Create A New Group Claim Extraction** window (Figure 5.21), click **Add** and click **Advanced**.

Figure 5.21 The Create A New Group Claim Extraction Window

4. Click **Object Types**, remove the checkmarks from everything except **Groups**, and then click **OK**.
5. Click **Find Now**.
6. Select **Domain Admins** from the list of groups by double-clicking.
7. Click **OK**.
8. The **Map To This Organization Claim** field should show the claim we created earlier. Click **OK** to close the window.

Finally, we will work to create the partner information of our resource partner, which is preguides.ads.

1. Expand **Partner Organizations**.
2. Right-click **Resource Partners**, and then select **New | Resource Partner**.
3. Click **Next** on the **Welcome** window.
4. We will not be importing a policy file, so click **Next**.
5. In the **Resource Partner Details** window (Figure 5.22), enter a friendly name for the partner, and the URI and URL information of the partner. When the information is complete, click **Next**.

Figure 5.22 Resource Partner Details

6. Click **Next** on the **Federation Scenario** page. This is the default selection, which is used for two partners from different organizations when there's no forest trust.
7. On the **Resource Partner Identity Claims** page, check **UPN Claim** and click **Next**. A UPN Claim is based on the domain name of your Active Directory structure. In our case, the UPN is `uccentral.ads`.
8. Set the UPN suffix. Verify that **Replace All UPN Suffixes With The Following:** is selected and then enter your server's domain name. This is how all suffixes will be sent to the resource partner. Click **Next**.
9. Click **Next** to enable the partner.
10. Click **Finish** to close the wizard.

We're almost at the end of our account partner configuration. The last thing we need to do is create an outgoing claim mapping. This is part of a claim set. On the resource side, we would create an identical incoming claim mapping.

1. **Expand Resource Partners.**
2. Right-click your resource partner, and then choose **New | Outgoing Group Claim Mapping**.
3. Select the claim we created earlier, enter **PrepGuide Mapping**, and then click **OK**.

As you can imagine, this process would be duplicated on the resource domain, with the exception that the outgoing claim mapping would be replaced with an incoming mapping.

Application Authorization Interoperability

Stretching application boundaries is not always possible. Maybe your organization does not have the resources to create and manage trust relationships (even when they are built using Web Services), or your customers simply do not support the creation of trusts or federation scenarios. In either scenario, you have to come up with a solution if your business requires remote users to access applications or services from your organization.

As with any external access, security is a key factor to keep in mind when you design an extranet solution. From a security point of view, application integration in Active Directory might be a risk if the application is accessed from outside the company. Therefore, other solutions must be used to authenticate and authorize remote users to applications and services provided by your organization. In this section we will talk about Active Directory Lightweight Directory Services as an authentication and authorization directory.

Using Active Directory Lightweight Directory Services to Provide Authentication and Authorization to Extranet Users

Formerly known as Windows Server 2003 Active Directory Application Mode (ADAM), ADLDS is a Lightweight Directory Access Protocol (LDAP) directory service that provides flexible support for directory-enabled applications, without the dependencies required for Active Directory Domain Services (ADDS). ADLDS provides much of the same functionality as ADDS, but does not require the deployment of domains or domain controllers.

Active Directory Lightweight Directory Service is a slimmed-down version of AD. The concept of LDS is not new. In fact, it has been around for several years. However, to date it is probably not as widely known or recognized as the full ADS

installation. Now that ADLDS is a part of the Windows Server 2008 media, you can expect to see many more deployments of the product.

When to Use AD LDS

So, when should you use ADLDS? Well, there are many situations when this is a more viable option. Typically, LDS is used when *directory-aware applications need directory services, but there is no need for the overhead of a complete forest or domain structure*. Demilitarized Zones (DMZs) are a great example of this. If you are not familiar with DMZs, Wikipedia defines a DMZ as a physical or logical sub network that contains an organization's external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN). You may be hosting an application or Web site in a DMZ where you want to have the added security of challenge/response using a directory services model. Since this is in a DMZ, you probably have no need for organizational units, Group Policy, and so on. By using LDS, you can eliminate these unnecessary functions and focus on what really is important: authentication and access control.

The other popular option for using LDS is in a situation where you want to provide authentication services in a DMZ or extranet for internal corporate users. In this scenario, account credentials can be synchronized between the full internal domain controller and the LDS instances within the DMZ. This option provides a single sign-on solution, as opposed to the end user being required to remember multiple usernames and passwords.

Changes from Active Directory Application Mode (ADAM)

As mentioned earlier, the LDS concept has been around since Windows Server 2003 R2, but many improvements and new features have been introduced since the previous release. Some of the key changes between ADAM and LDS are listed next:

- **Auditing** Directory Service changes can now be audited for when changes are made to objects and their attributes. In this situation, both old and new values are logged.
- **Server Core Support** ADLDS is now a supported role for installation in a Server Core implementation of Windows Server 2008. This makes it ideal for DMZ-type situations.

- **Support for Active Directory Sites and Services** This makes it possible for management of LDS instance replication using the more-familiar ADS&S tool.
- **Database Mounting Tool** Provides a means to compare data as it exists in database backups that are taken at different times to help the process of deciding which backup instance to restore.

These are the key improvements from ADAM in Windows Server 2003 R2 to ADLDS in Windows Server 2008, but the fact that the product has had more time to be “baked in” will greatly improve the functionality and usage of this technology.

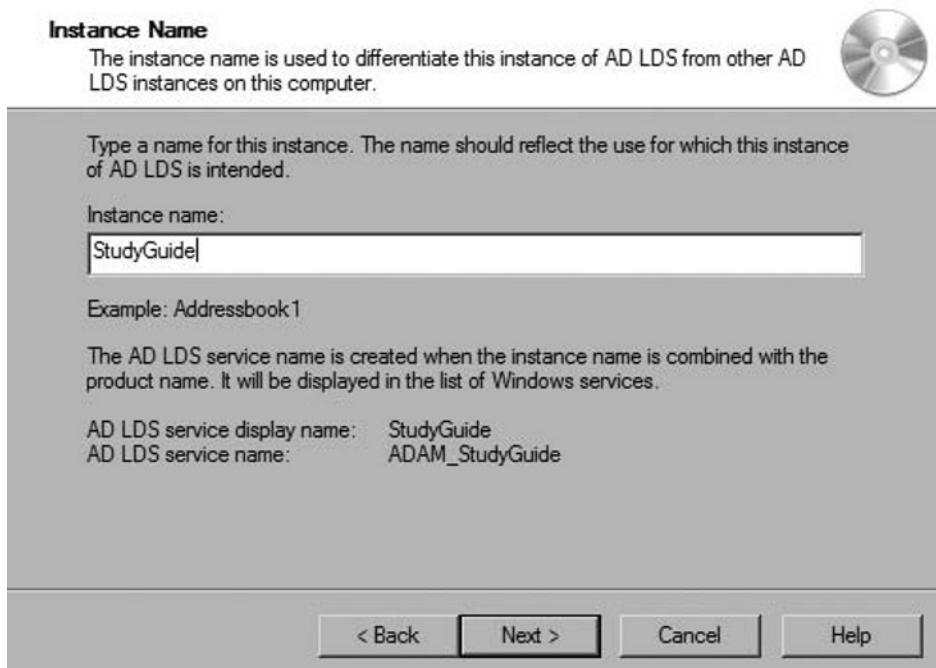
Configuring AD LDS

By now, you’re probably beginning to see a trend in how things are accomplished in Windows Server 2008. Everything is done with the use of server roles. Active Directory Lightweight Directory Services are no different. In our example, we are going to walk through the process of installing a clean LDS implementation.

EXERCISE 5.11

CONFIGURING LDS

1. Choose **Start | Administrative Tools | Server Manager**.
2. Scroll down to **Role Summary**, and then click **Add Roles**.
3. When the **Before You Begin** page opens, click **Next**.
4. On the **Select Server Roles** page, select the **Active Directory Lightweight Directory Services** option, and then click **Next**.
5. The installation steps for the role are very straightforward: follow the prompts and then click **Install**. After the role installation is complete, move on to creating an LDS instance.
6. Select **Start | Administrative Tools | Active Directory Lightweight Directory Services Setup Wizard**.
7. On the **Welcome** page, click **Next**.
8. On the page, select **A Unique Instance**, and then click **Next**.
9. On the **Instance Name** page (Figure 5.23), provide a name for the ADLDS instance and click **Next**.

Figure 5.23 The Instance Name Page

10. On the **Ports** page, we can specify the ports the ADLDS instance uses to communicate. Accept the default values of 389 and 636, and then click **Next**.
11. On the **Application Directory Partition** (Figure 5.24) page, we will create an application directory partition by clicking **Yes**.

Figure 5.24 The Application Directory Partition Page

12. On this page, we will also need to specify the distinguished name of our partition. Follow the format in Figure 5.24, and then click **Next**.
13. On the **File Locations** page, review the file locations and click **Next** to accept the default locations.
14. On the **Service Account Selection** page, select an account to be used as the service account. By default, the Network Service account is used. Click **Next** to accept the default option.
15. On the **AD LDS Administrators** page (Figure 5.25), select a user (or group) that will be used as the default administrator for this instance. Click the default value (**Currently Logged On User**) and then click **Next**.

Figure 5.25 The AD LDS Administrators Page

16. Select particular LDIF files to work with our LDS implementation. We will use the MS-ADLDS-DisplaySpecifiers file later in this section, so check this option off, and then click **Next**.
17. Review the **Ready To Install** page and click **Next** to begin the installation process. When setup is complete, click **Finish**.

Working with AD LDS

Several tools can be used to manage an LDS instance. In this book, we will work with two of these tools. The first is the ADSI Edit tool. ADSI stands for Active Directory Service Interfaces, and is used to access the features of directory services from different network providers. ADSI can also be used to automate tasks such as adding users and groups and setting permissions on network resources. While making changes to LDS (or Active Directory) is outside the scope of this book, we will show you how to use ADSI Edit to connect to an LDS instance.

1. Choose **Start | Administrative Tools | ADSI Edit**.
2. In the console tree, click **ADSI Edit**.
3. On the **Action** menu, click **Connect to**.
4. In the **Name** field, type a recognizable name for this connection. This name will appear in the console tree of ADSI Edit.
5. In **Select Or Type A Domain Or Server**, enter the fully qualified domain name (or IP address) of the computer running the ADLDS instance, followed by a colon and 389—representing the port of the LDS instance.
6. Under **Connection point**, click **Select** and choose your distinguished name, then click **OK**.
7. In the console tree of the ADSI Edit snap-in, double-click the name you created in step 4, and then double-click the distinguished name of your LDS instance.
8. Navigate around the containers to view the partition configuration.

The second tool we will discuss is the Active Directory Sites and Services snap-in. As mentioned earlier in this section, you can use the ADS&S snap-in to manage replication of directory information between sites in an LDS implementation. This is useful when LDS may be implemented in a geographically disbursed environment. For example, a server farm that may be collocated in a company datacenter and a disaster recovery location may require replication, and the easiest way to perform this is via this snap-in. However, it's important to note that we *must* import the MS-ADLDS-DisplaySpecifiers.ldf file during the instance configuration (earlier in this section) in order to use ADS&S. Let's review how to use ADS&S to connect to an LDS instance.

1. Choose **Start | Administrative Tools | Active Directory Sites & Services**.
2. Right-click **Active Directory Sites and Services**, and then click **Change Domain Controller**.
3. In the **Change Directory Server** window, type the FQDN or IP address of the server running the LDS instance, followed by 389.
4. Navigate the containers to view information about the LDS instance.

Cross-Platform Interoperability

In heterogeneous networks it is common to require interoperability software. Access to resources, user and group administration, password management, and more—you have to manage them in the most effective way. From a client/server perspective there are two approaches to this. On one hand you could install an interoperability software on all foreign systems to access resources on Windows Servers, or on the other hand you could install interoperability software on your Windows Server so that they emulate the functionality of a foreign system. In this section we will talk about interoperability between Windows operating systems and other, mainly Unix-based, operating systems.

Windows Server 2008 includes several services to interoperate with other platforms. Active Directory for example is built on standards such as LDAP, DNS, and Kerberos, technologies that interoperate with any client or server platform that is designed to support these standards. Especially for interoperability with Unix-based systems, Windows Server 2008 includes additional services, which you can install on demand. These include the Identity Management for Unix Role Service and the Services for Network File System Role Service.

File System Paths and Permissions on Unix Systems

File system and network paths on a Unix System are separated by a forward-slash (/) in comparison to the back-slash (\) that is used on Windows systems, and drive letters do not exist. An example: your home folder on a Windows System may be C:\Users\Username\Documents. On a Unix system this folder structure would be presented as /Users/Username/Documents. This notation is also used by the Network File System (NFS) which we describe later in this chapter. Working with NFS, you *mount* a network path into a local folder, therefore creating a virtual representation of the network resource on your local machine. The path /Users/Username/Documents from the previous example could also be located on a network server.

It is important to mention that file system permissions on a Unix-like system work different than on Windows systems. Classical Unix file system permissions are not as powerful as NTFS Access Control Lists. Permissions are managed in three distinct classes: user, group, and others.

Every file or directory is owned by a specific user. The user class comprises the object owner. Permissions assigned to the user class only apply to that user. Groups are also assigned to a file or directory which in turn comprises its group class. Permissions assigned to the group only apply to members of that group. All other users who are not represented by the other classes comprise a file's *others* class.

Unix-like systems use three specific permissions, each of which applies to each class: the read permission, the write permission and the execute permission. The read permission grants the ability to read a file. When set for a directory, it grants the ability to read the names of files in the directory. The write permission grants the ability to modify a file. When set for a directory, this permission grants the ability to create, delete, and rename entries in the directory. The execute permission grants the ability to execute a file. When set for a directory, this permission grants the ability to traverse its tree in order to access files or subdirectories, but not see files inside the directory (unless read is set). Permissions on a Unix-like system are not inherited.

Authentication on Unix Systems

Unix systems provide a wide variety of authentication mechanisms. Users and Groups are identified by a UID (user ID) or a GID (group ID) compared to the SID on Windows Systems. The standard mechanism on a Unix System is authentication based on entries in a local file */etc/passwd* where user information is stored. Passwords are stored in the file */etc/shadow*, which is only readable by the administrator of the system (on Unix systems the *root* account). However, on modern Unix Systems so-called Pluggable Authentication Modules (PAM) are used to allow the use of several different authentication mechanisms such as Network Information System (NIS), LDAP, or Kerberos.

Network Information System

NIS was developed by Sun Microsystems to centralize administration of UNIX systems and is the quasi de-facto industry standard for authentication on Unix systems since all major UNIX-like systems support NIS. It was formerly known as Yellow Pages, therefore the old term (and the command *yp*) is still often seen and used. Similar to Windows Domains, NIS is a client/server system that allows a group of machines within an NIS *domain* to share a common set of configuration files. There are three types of hosts in an NIS environment: master servers, slave servers, and clients. Comparable to Domain Controllers, Servers act as a central repository for host configuration information. Master servers hold the authoritative copy of this information, while slave servers mirror this information for redundancy. Clients rely on the servers to provide this information to them.

Information stored on servers includes usernames, passwords, hosts files, and more. Unlike Windows Domain Controllers, NIS Servers share that information, meaning that if a client needs to look up an entry in the host's file it will do the lookup on the NIS Server.

NIS+

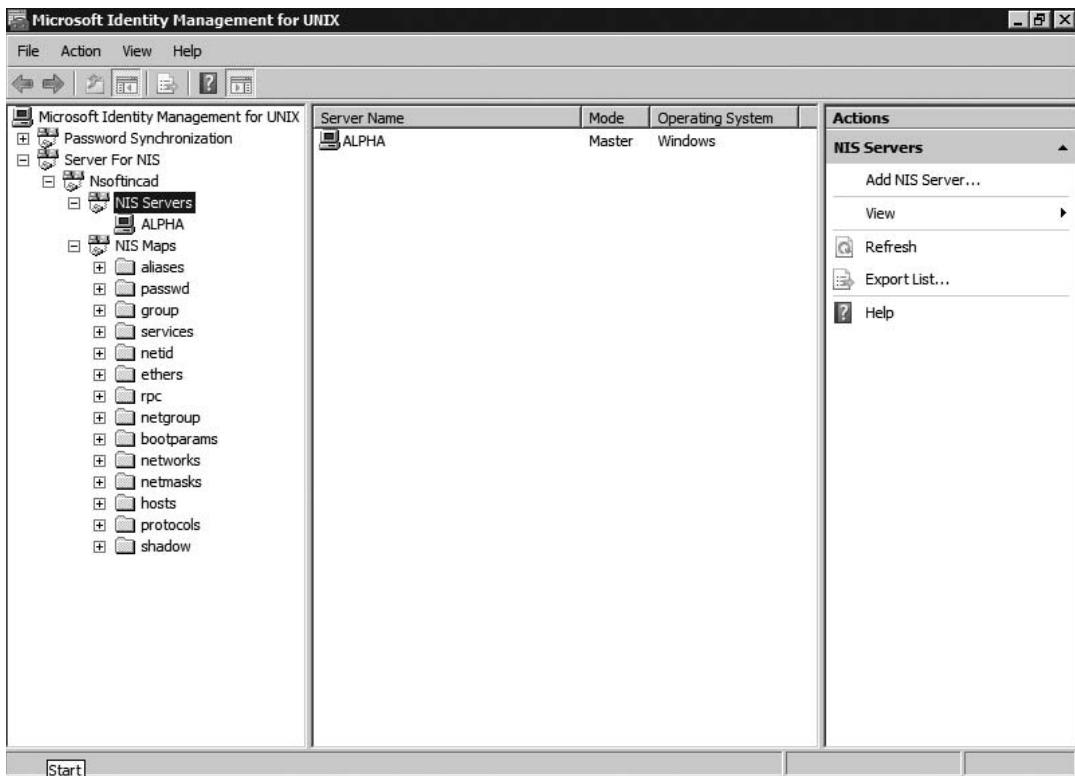
NIS+ is a directory service also developed by SUN Microsystems and is not considered the successor of NIS. Unlike NIS it uses a hierarchical structure based on Secure RPC and implements permissions on the directory service.

Windows Server 2008 includes the Identity Management for Unix Role Service to better integrate Unix-based clients and servers that are Kerberos enabled into an Active Directory infrastructure. Identity Management for Unix, which was formerly known as Service for Unix, includes a Server for NIS component that allows a Windows Server to act as a NIS Master server. NIS Domain maps are exported on the NIS Master Server and then imported into Active Directory. Admin-Extension to Active Directory Users and Computers allow the administrator to configure Unix-Attributes such as the UID, GID, home directory, and others.

To minimize the overhead of credential management, a password synchronization service is also included. The service can be configured to update user passwords on Unix hosts when a user changes the password in Active Directory or vice versa. To maintain the integrity of user passwords the service transfers them encrypted. Figure 5.26 shows the Identity Management for Unix Management Console.

NOTE

Even though NIS is a very popular authentication service on UNIX systems, it is more and more replaced by LDAP directory services and alternative authentication protocols such as Kerberos. Also vendors recommend their customer the use of an LDAP directory instead of NIS or NIS+.

Figure 5.26 Identity Management for Unix MMC

EXERCISE 5.12

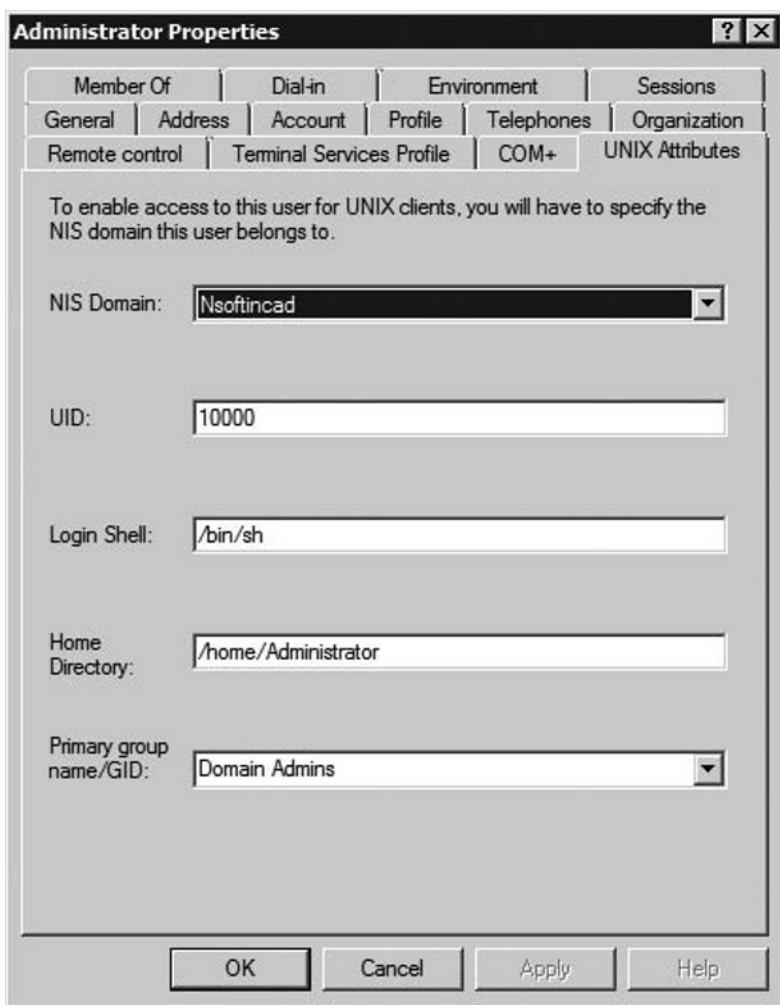
INSTALLING IDENTITY MANAGEMENT FOR UNIX

1. Log-on as administrator to a Windows Server 2008 domain controller.
2. Click **Start | Administrative Tools | Server Manager**.
3. In the console tree open the **Roles** node, right-click **Active Directory Domain Services** and select **Add Role Services**.
4. On the **Select Role Services** page, select **Identity Management for Unix** from the list and click **Next**.
5. On the **Confirm Installation Selections** page, click **Install**.

EXERCISE 5.13

CONFIGURING UNIX ATTRIBUTES ON ACTIVE DIRECTORY ACCOUNTS

1. Log on as administrator to a Windows Server 2008 domain controller where Identity Management for Unix is installed.
2. Click **Start | Administrative Tools | Active Directory Users and Computers**.
3. In the console tree expand the **domain node** and the click on the **Users** container.
4. In the results pane right-click the **administrator** account and select **Properties**.
5. In the **Properties** window, select the **UNIX Attributes** tab.
6. Click on the **NIS Domain** drop-down list and select an **entry**.
Normally there is an entry for your Active Directory Domain. This will automatically fill out the remaining fields and generate a Unix User ID (UID) starting with 1000. Figure 5.27 shows the completely data-filled user property dialog.

Figure 5.27 Unix Attributes on a User Account in Active Directory

Network File System (NFS)

NFS is a network file system protocol that allows users on clients to access files on network servers as easily as if the files were located on the local system. It was initially developed by SUN Microsystems in 1984 for in-house use but in 1989 was also defined as RFC 1094 which was jointly developed with IBM. Originally specified as Version 2, NFS was later revised in 1995 (Version 3, RFC 1813) and 2000/2003 (Version 4, RFC 3510 and RFC 3530).

Version 2 is a stateless protocol and operates over UDP only. Beginning with Version 3, TCP is supported as a transport and enhancements were made in the

areas of performance, security, and support for large file structures (64 bit support). Version 4, which was the first version developed with the Internet Engineering Task Force (IETF) mandates security, includes performance improvements, and defines a stateful protocol.

EXAM WARNING

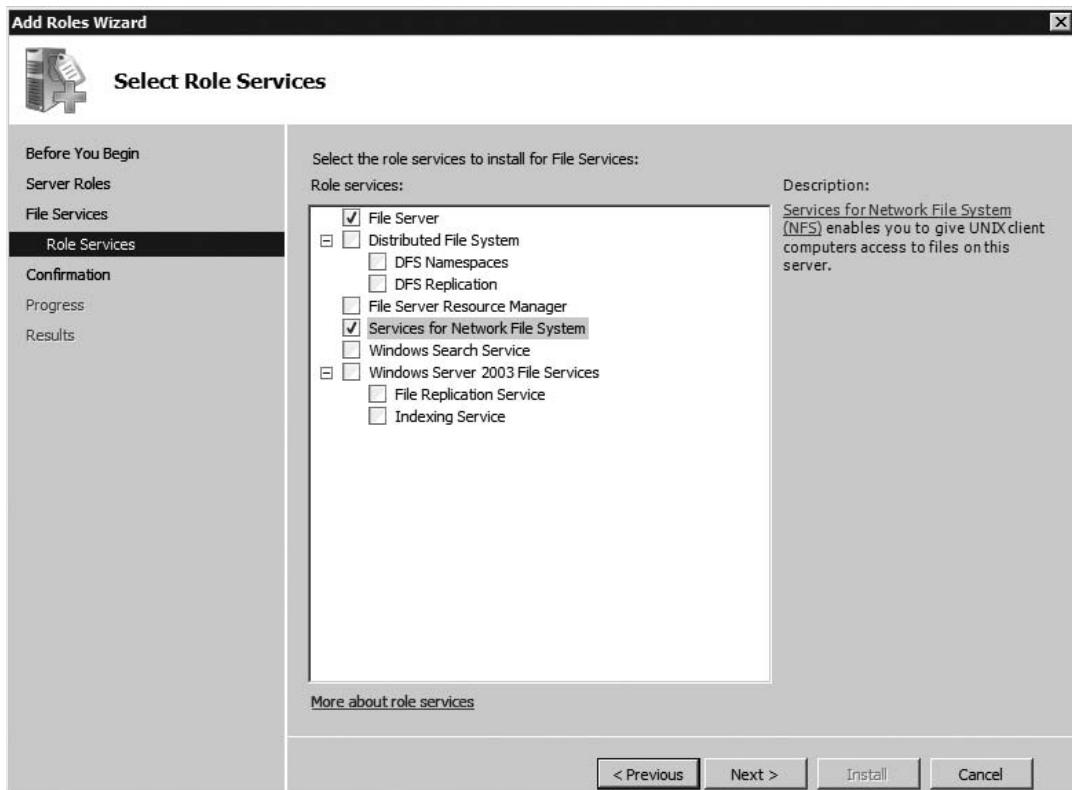
Microsoft developed an updated version of the Server Message Blocks (SMB) protocol, which is used for file-sharing, for Windows Vista and Windows Server 2008. SMB 2.0 includes support for symbolic-links. Symbolic-links allow you to map a Network Share to a local folder just like NFS does. To create symbolic-links, you use the **mklink** tool on the command line.

In the following exercises you will install and configure Services for NFS, create shares that are available to NFS clients, and assign UNIX-like permissions on those shares.

EXERCISE 5.14

INSTALLING SERVICES FOR NFS

1. Click **Start | Administrative Tools | Server Manager**.
2. Scroll down to **Role Summary**, and then click **Add Roles**.
3. When the **Before You Begin** page opens, click **Next**.
4. On the **Select Server Roles** page, select **File Services** from the list and click **Next**.
5. On the **Select Role Services** page, select services for **Network File Service** (See Figure 5.28) and click **Next**.

Figure 5.28 Selecting the Services for Network File Service Role

6. On the **Confirm Installation Selections** page, click **Install**.

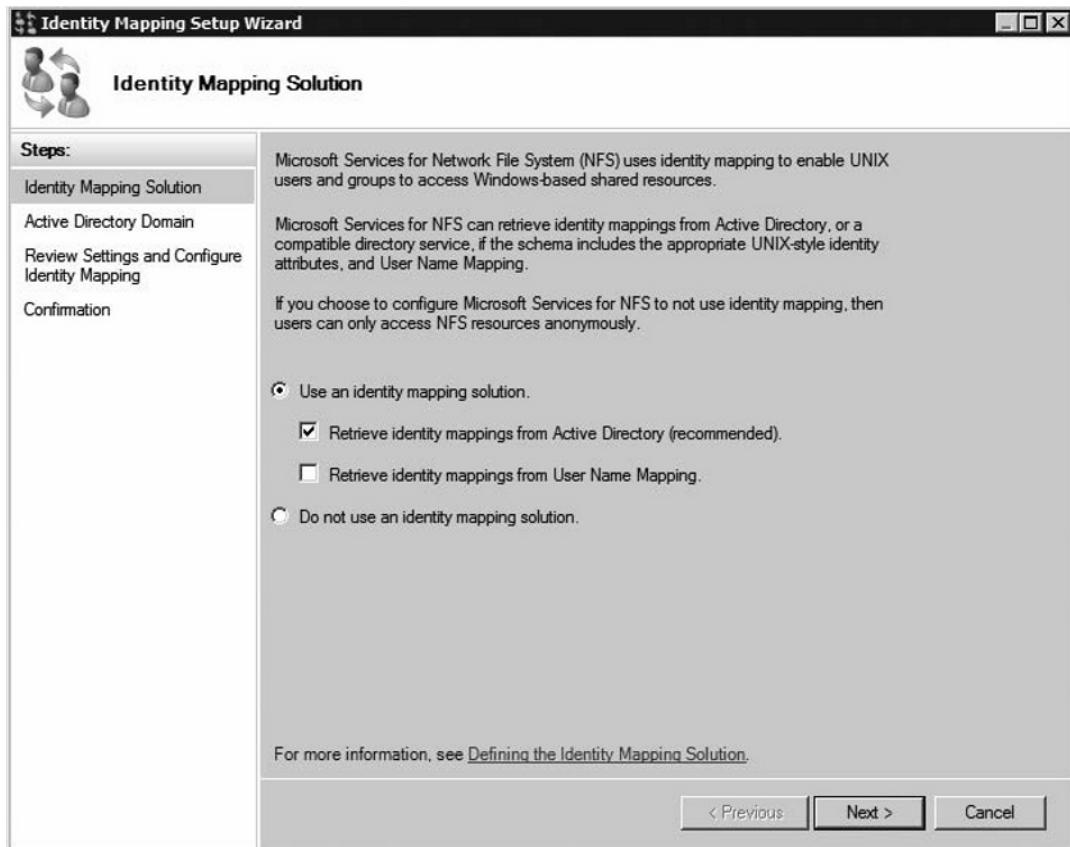
EXERCISE 5.15

CONFIGURING SERVICES FOR NFS

1. Click **Start | Administrative Tools | Server Manager**.
2. In the console tree click **Roles**, expand **File Services**, and then expand **Share and Storage management**.
3. Right-click the **Share and Storage management** node and select **Edit NFS configuration....**
4. In the **Microsoft Services for NFS Configuration Guide** window, select **Select and Identity Mapping Solution**.
5. Click the **Identity Mapping Wizard** button in the **results pane** to start the **Identity Mapping Setup Wizard**.

6. On the **Identity Mapping Solution** page, select the **Retrieve identity mappings from Active Directory (recommended)** checkbox (see Figure 5.29) and click **Next**.

Figure 5.29 Selecting an Identity Mapping Solution



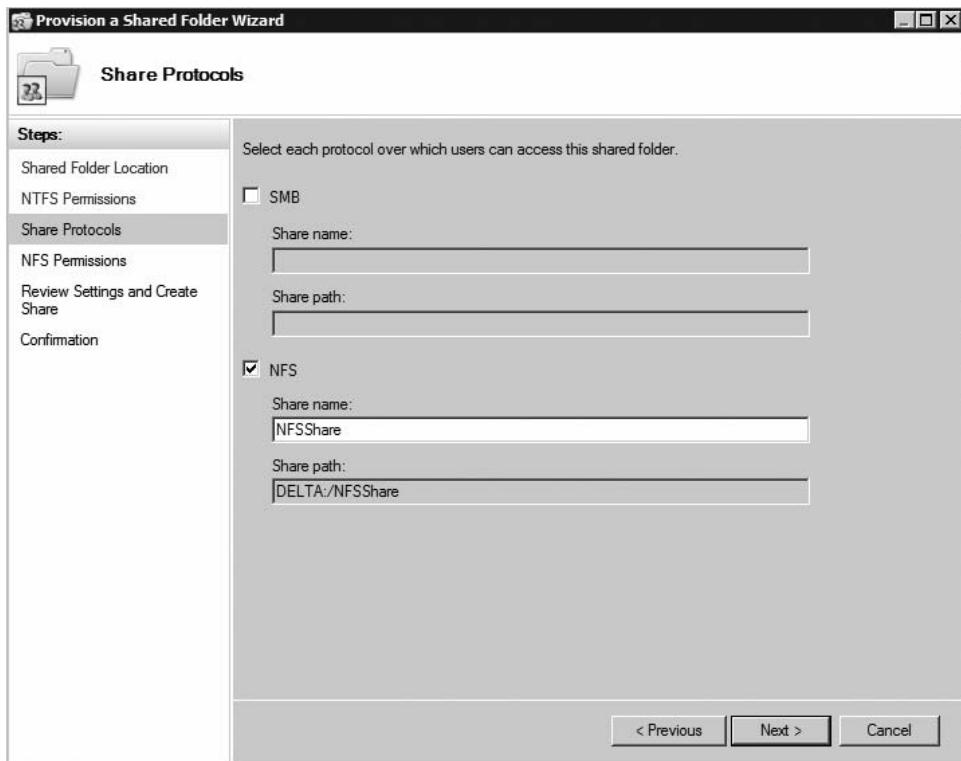
7. On the **Active Directory Domain** page, type the name of your Active Directory domain and click **Next**.
8. On the **Review Settings and Configure Identity Management** page click **Configure**.
9. On the **Confirmation** page click **Close**.
10. Click **Close** to close the Microsoft Services for NFS Configuration Guide window.

EXERCISE 5.16

CREATING A NFS FILE SHARE

1. Click **Start | Administrative Tools | Server Manager**.
2. In the console tree click **Roles**, expand **File Services**, and then expand **Share and Storage management**.
3. Right-click the **Share and Storage management** node and select **Provision Share....**
4. On the **Shared Folder Location** page, click **Browse...**, select **C\$**, click **Make New Folder**, type **NFSShare**, click **OK**, and then click **Next**.
5. On the **NTFS Permissions** page, select **No, do not change NTFS permissions** and click **Next**.
6. Select the **NFS** checkbox on the **Share Protocols** page and click **Next** (see Figure 5.30).

Figure 5.30 Selecting NFS as File Sharing Protocol



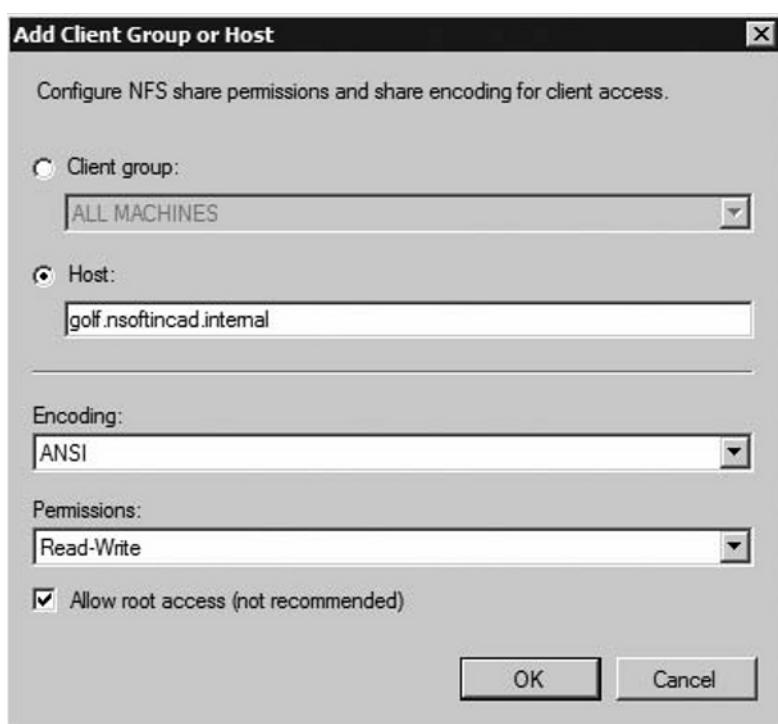
7. On the **NFS Permissions** page click **Next**.
 8. Click **Create** on the **Reviewing Settings and Creating Share** page.
 9. On the **Confirmation** page click **Close**.
-

For security reasons, root access to NFS shared folders is not enabled on Windows systems by default. In the next exercise you will add root access permissions to the previously created NFS share for an administrative workstation.

EXERCISE 5.17

ADDING A ROOT ACCESS ENTRY TO A NFS SHARE

1. Click **Start | Administrative Tools | Server Manager**.
2. In the console tree click **Roles**, expand **File Services**, and then expand **Share and Storage management**.
3. In the **results pane** locate the share that you previously created under **Protocol: NFS**, right-click the share, and select **Properties**.
4. In the **NFS Share Properties** dialog, select the **Permissions** tab and click **NFS Permissions**.
5. Click **Add** in the permissions window.
6. In the **Add Client Group or Host** window, select the **Host:** radio button and type in a hostname.
7. From the **Permissions** drop-down list select **Read-Write**, select the **Allow root access (not recommended)** checkbox, click **OK** (see Figure 5.31).

Figure 5.31 Adding a Host Entry to the List of NFS Share Permissions

8. In the Permissions windows click **OK**, and then click **OK** to complete the configuration.
-

Summary of Exam Objectives

When companies upgrade or migrate their infrastructures to a new operating system version, the driving factors are business and/or technical related.

You can use the upgrade or restructuring method to update your Active Directory infrastructure to a new operating system version. An upgrade preserves the existing topology. To upgrade your existing forest you first have to extend the Schema and prepare each Domain for the installation of Windows Server 2008 domain controllers. Installation of Read-only domain controllers requires additional steps.

There are two methods for restructuring, Intra-Forest and Inter-Forest. In Intra-Forest restructuring, you move objects between domains inside an existing forest. Intra-Forest restructuring allows you to reduce the number of domains and lowers the administrative overhead. An Inter-Forest restructure requires a separate, new forest to which objects are cloned. Cloning creates new objects in the target forest and duplicates properties from the old object. The cloning process allows you to revert your changes, as it does not change the original object.

To maintain resource access during a restructure, you should consider the use of SID History. SID History is an additional attribute on user and group objects in Active Directory. During migration, the accounts' old SID is copied to the SID History attribute of the new account. Access to resources in the source forest is maintained by checking the SID-History. To use SID History, your target forest or domain must be at least running in Windows 2000 native mode. Tools such as ADMT provide the necessary functionality to update the SID History attribute. Do not forget to configure your trusts to allow for SID History evaluation.

Object migration should begin with the cloning of groups. When you clone groups, do not duplicate group membership. Group membership will be fixed when users are migrated. Before you clone user accounts, plan for a password migration strategy. ADMT provides the Password Export Server service to copy passwords from the source to the target forest. The last step would be to migrate computer accounts. You cannot clone computer accounts; therefore, you need to change domain membership. To automate this process, ADMT provides an agent that installs locally on computers and automatically changes domain membership. If demanded, the agent also translates security and local user profiles.

Your Active Directory migration plan should be separated into distinct phases. Microsoft offers a Solutions Framework (MSF) as guidance for IT projects. According to MSF, you should separate your project into the following phases:

- Envisioning
- Planning
- Developing
- Stabilizing
- Deployment

Web Services have their roots in the HTTP protocol, which they extend. They define extension for security, reliable messaging, and exchange of security tokens over a standard HTTP channel. Web Service Standards are also referred by the name WS-*¹. WS-* enables companies with different operating system platforms to build a trust relationship and to federate. Federation is often used in business to business (B2B) and business-to-customer (B2C) scenarios. In a federation scenario the involved parties are referred to as Account Partner (the company that manages identities) and Resource Partner (the company that offers a service).

Active Directory Federation Service (ADFS) is built on Web Service protocols and provides support for federation across organizations. ADFS is a role on Windows Server 2008 and requires either Active Directory Domain Services or Active Directory Lightweight Directory Service for installation. ADFS enabled Web-Applications use the ADFS Web agent that must be installed on IIS to authenticate users.

If you do not want external users to use your Active Directory as an authentication directory for an extranet application, Active Directory Lightweight Directory Services (AD LDS) provides a viable alternative. AD LDS is a slimmed-down version of Active Directory with fewer requirements for installation but similar functionality. Formerly known as ADAM, it is now a role of Windows Server 2008. Improvements to AD LDS include auditing, server core support, support for active directory sites and services, and a new tool to mount AD LDS databases. You manage AD LDS with the ADSIEDIT MMC snap-in or from the command line.

UNIX-based systems handle user authentication and file system permissions different from Windows systems. On UNIX-based systems, by default, local users exist in the file */etc/passwd* and passwords are stored in the file */etc/shadow*, which is only readable for the root account. Pluggable Authentication Modules allow you to use authentication modules for any authentication protocol and therefore provide more flexibility.

Traditional permissions on a UNIX-based system are not as powerful as NTFS permissions. Permissions are managed in three classes: user, group, and other. You assign three different permissions to these classes: read, write, and execute, which can be individually assigned for folders and files. Unlike NTFS Access Control Lists, permissions are not inherited.

Network File System (NFS) allows you to access a network resource via a local folder path. NFS is widely used and there are four version of the protocol. Version 2 is a UDP only, stateless protocol, and Version 3 and 4 both add improvements in the areas of performance and security. Windows Server 2008 includes Services for NFS to allow a Windows Server 2008 to act like a NFS Server, or to access resources on a host that offers NFS resources.

Network Information System (NIS) is a central repository that provides authentication and configuration services for UNIX-based systems. Despite the name, NIS+ is not the successor of NIS. It implements a directory service and also provides authentication and configuration services for UNIX-based systems. Both NIS and NIS+ are more and more replaced by other technologies such as LDAP directories and the Kerberos protocol. To provide UNIX authentication services, Windows Server 2008 includes the Identity Management for UNIX Role Service which emphasizes a Server for NIS component, a password replication service, and extensions for Active Directory Users and Computers. With Server for NIS a Windows Server 2008 acts like a NIS Master Server. The password replication service synchronizes passwords between UNIX-based systems, and the Active Directory Users and Computers extensions allow the administrator to edit UNIX attributes on user and group objects.

Exam Objectives Fast Track

Planning for Migration, Upgrades, and Restructuring

- Upgrades and restructures are driven by business needs
- Intra-Forest migration and Inter-Forest migrations are two restructuring methods
- ADMT is a tool that allows for restructuring
- You should use SID History in a restructuring scenario to maintain resource access
- As a best practice migration planning is separated into distinct phases
- Cross-Forest authentication requires creation and management of trusts

Planning for Interoperability

- Interoperability between Web Services are based on the HTTP protocol and define extensions for security, reliable messaging, and embedding of security tokens.

- Active Directory Federation Service (ADFS) is based on Web Services and allows companies to collaborate in various ways.
- Active Directory Lightweight Directory Service (ADLDS) is an application directory that provides authentication and authorization for directory enabled applications. Extranet authentication is a typical application for ADLDS.
- Network File System (NFS) is a network file system used on UNIX-based systems.
- Services for NFS allow a Windows Server to act as a NFS Server and Client.
- Network Information System (NIS) and NIS+ centralize administration for UNIX systems. Besides user authentication, they also provide a central repository for configuration items.
- Identity Management for UNIX is a Windows Server 2008 Role Service that provides NIS Server facilities for Windows Server and implements a password replication service.

Exam Objectives

Frequently Asked Questions

Q: I did not read anything about Windows NT4 domains in this book. How can I upgrade from Windows NT4 to Windows Server 2008?

A: Since Windows NT4 is no longer supported by Microsoft, you cannot in-place upgrade to Windows Server 2008. The only way would be a restructuring to a new forest.

Q: Is it possible to change the forest root domain during an intra-forest restructure?

A: No, unfortunately this is not possible. The forest root domain is established during promotion of the first domain controller in the first domain and cannot be changed.

Q: When I use ADMT, is it possible to move a Domain inside the forest structure?

A: No, Microsoft does not support moving domains. Moving domains would imply removing default trust relationships, which is not possible with current technology.

Q: Can I populate the SID History attribute with the SID of an administrative group, such as Enterprise Admins? This would allow for privilege escalation.

A: Tools provided by third parties do not support this kind of operation. However, there are hacking tools available that allow such modifications. Therefore, physically securing your domain controllers is an important task!

Q: I tried to migrate Windows XP computers from one forest to another. Unfortunately, the migration failed with the error message *unable to ping remote host*.

A: This is a common error when migrating Windows XP hosts. Because the firewall is enabled by default in Windows XP Service Pack 2, the ADMT cannot connect to the machine and install the agent.

Q: Since ADLDS does not have the same dependencies as ADDS, how can I install multiple instances of ADLDS on the same computer?

A: To create multiple instances of ADLDS on the same computer, you must ensure that every instance of ADLDS is configured to use a unique combination of IP Address and TCP Port.

Q: How do I replicate information between two instances of ADLDS on different computers?

A: There are two ways to accomplish this. Either you create a replica instance of the source ADLDS instance by using the Active Directory Lightweight Directory Services Setup Wizard, or you install ADLDS by using install from media technology. Install from media setup is started with the command **%windir%\adam\adaminstall /adv.**

Q: How can I replicate information from ADDS to ADLDS?

A: First, you have to import parts of the schema of Windows Server 2008 ADDS and then you use **adamsync** to synchronize objects.

Q: I installed the Identity Management for UNIX Service on my domain controller. However, I am not able to edit UNIX attributes in Active Directory Users and Computers from other servers.

A: To see the UNIX attributes tab in Active Directory Users and Computers, you must install the “Server for NIS Tools.” They are part of the Remote Server Administration Tools feature and can be installed by using Server Manager.

Q: Are there any tools to automate the creation of NFS shares in Windows Server 2008?

A: Yes, you can use the command line tool **nfsshare** to create and modify NFS shares.

Q: How does Windows Server 2008 store UNIX attributes in Active Directory?

A: Windows Server 2008 Active Directory includes Schema extensions to store UNIX attributes.

Self Test

1. You want to upgrade your existing infrastructure to Windows Server 2008. Which factors should influence your upgrade?
 - A. Time constraints
 - B. Resource availability
 - C. Budget
 - D. Application compatibility
2. Simon is in the process of an intra-forest restructuring of his Active Directory. He wants to maintain user passwords during the migration. For this purpose he installs the PES service on one of the domain controllers in the source domain. When he selects the **Migrate passwords** option in ADMT and clicks **next**, an error occurs stating that PES service cannot be contacted in the source domain. What could be the cause for this error? (Select all that apply)
 - A. Password migration is not supported in an intra-forest migration.
 - B. He didn't install the PES Service on the PDC Emulator FSMO role holder.
 - C. He didn't set the **AllowPasswordExport** Registry value to **1** on the PES.
 - D. He must be a member of the **AllowPasswordExport** group in the source domain.
3. You decided to install a new Windows Server 2008 domain controller into your existing Windows Server 2003 Active Directory. What tasks do you have to complete before installing the first Windows Server 2008 Domain Controller?
 - A. Raise the forest functional level to Windows Server 2003
 - B. Extend the Active Directory Schema
 - C. Prepare the Domain
 - D. Pre-stage the Domain Controller account in Active Directory
4. Your company is operating a Windows Server 2008 Active Directory. The Forest is operating at Windows Server 2008 functionality level. Your boss tells you to install an additional Windows Server 2003 domain controller into the domain because of some application compatibility issues. When you try to install the new domain controller, you fail. What could be the reason for your failure?

- A. You didn't use the **/adv** switch when running DCPROMO.
 - B. You cannot add Windows Server 2003 domain controllers to a forest that is operating at Windows Server 2008 functionality mode.
 - C. Your Windows Server 2003 domain controller is not running Service Pack 2.
 - D. You didn't enable the Windows Server 2003 compatibility flag on the domain where you try to install the new domain controller.
5. Mark is in the middle of a migration to a new Active Directory Forest. Recently he migrated the first bulk of users by using ADMT. However, when users log on with the new account, they cannot access resources in the old forest. He examines the user accounts in Active Directory and discovers that the SID History is correctly populated. What else must he do to allow resource access with SID History?
- A. Enable the **use SID History** flag in the source forest.
 - B. On the target forest, disable SID Filtering on the incoming trust.
 - C. Add the new user accounts to the access control list on servers in the source forest.
 - D. On the Source Forest, disable SID Filtering on the incoming trust.
6. Linda is migrating Users and Groups to a new forest using ADMT. After she migrates all of her user accounts, she discovers that the group membership is empty. What steps must she take before she migrates user accounts?
- A. Migrate groups first.
 - B. Export the group membership on the source forest and then import it on the target forest.
 - C. Select the **preserve group membership** checkbox in ADMT.
 - D. Do nothing, as this is by design.
7. Your company is restructuring the existing Active Directory. You want to install the Password Export Server (PES) Service on a domain controller in a source domain. You run the **admt /key** command to create the PES key. When you install PES, an error occurs stating that the key is not valid for this domain. What can be the cause for this error?
- A. PES cannot be used for Intra-Forest restructuring.
 - B. PES must be installed in the target domain.

- C. You must use a stronger encryption algorithm for the key.
 - D. The PES key must be created in the target domain.
8. Alan wants to restructure his Windows Server 2003 Active Directory Forest. He decided to build a new forest. The forest is operating at Windows Server 2008 forest functionality level. He uses ADMT Version 3 to migrate users, groups, and computers. When he starts with the group migration, ADMT fails to migrate accounts. Why isn't he able to migrate accounts?
- A. Migration between Windows Server 2003 and Windows Server 2008 is not supported.
 - B. He must use the version of ADMT specifically built for Windows Server 2008.
 - C. He must install at least one Windows Server 2008 domain controller in the source forest.
 - D. If you use ADMT Version 3, the target forest must not operate at Windows Server 2008 Forest functionality level and at least one Windows Server 2003 domain controller must be present.
9. Your boss tells you to use the Microsoft Solutions Framework (MSF) to manage your migration project. Which of the following phases are recommended by MSF?
- A. Envisioning
 - B. Strategy
 - C. Stabilizing
 - D. Deployment
 - E. Managing
10. Which of the following protocols does Web Services use?
- A. XML
 - B. SOAP
 - C. IPSEC
 - D. HTTP

Self Test Quick Answer Key

- | | |
|---------------|-------------|
| 1. A, B, C, D | 6. A |
| 2. B, C | 7. D |
| 3. B, C | 8. B, D |
| 4. B | 9. A, C, D |
| 5. D | 10. A, B, D |

Chapter 6

MCITP Exam 647

Designing a Branch Office Deployment

Exam objectives in this chapter:

- Developing an Authentication Strategy
- Using BitLocker
- Configuring Read-Only Domain Controllers

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

Branch office infrastructures have special requirements (or constraints) in addition to normal infrastructures, and are always a challenge for both architects and IT professionals. In this chapter, we will learn about these special requirements. We will also talk about how to design an authentication strategy with these requirements in mind.

Windows Server 2008 provides several features that support the administrator as well as the architect in supporting and deploying a branch office. Windows BitLocker can help in keeping data more secure and provides a robust recovery mechanism. You will learn the basics of BitLocker, how to install and configure BitLocker, and also how to configure Active Directory to back up BitLocker recovery information.

Due to its read-only Active Directory database, a Windows Server 2008 Read-Only Domain Controller (RODC) provides an additional layer of security for branch office deployments. We will discuss how RODC authentication and password replication works, and show you how to implement role separation. Finally, you will learn about the different methods to remotely administer a branch office.

The Branch Office Challenge

As mentioned before, a branch office deployment is a very special project. Infrastructure is deployed to many locations that are spread across a country or even a continent. One of the most important steps of a branch office deployment is the creation of an authentication strategy. But before we start, let's have a look at some of the factors that influence such a design.

Network Bandwidth

Ideally, all branches are connected with a high-speed link, and connections are stable and have excellent roundtrip times. Sounds like a fairy tale. In reality, branch offices often have a low speed-high latency wide area network link. Network links are expensive and the support service of the network provider is not the best. Bandwidth might also be shared by many different services and applications like ERP systems, telephony, directory services and so on.

Security

Security is always an important topic. Unfortunately, security in a branch office might not fulfill the “normal” requirements of a company. Often physical security

cannot be guaranteed, therefore making server systems an easy prey for thieves. Client systems are not as easy to control as if they were located in a central office. How do you prevent a user from introducing an unwanted device into the network (or even the server “room”)? Even if you define policies and procedures for a branch office, who is there to enforce them?

Backup and Restore

The availability and recoverability of data is a major goal when companies design their computing environments. In a branch office scenario, you need to consider additional factors when you design a backup strategy. Well-known technologies such as tapes or optical discs possibly will not fit because they require human interaction. Moreover, most branches are too small for automated systems such as automated tape libraries. Requiring human interaction also implicates that you need a trusted person to maintain and store backup media. This person needs to be educated and will have access to server systems to some extent.

Several other or newer technologies exist to cope with these problems. Windows Server 2008 itself ships with a feature that is a perfect replacement for old-fashioned backup media in remote locations, called *Distributed File System Replication (DFS-R)*. Introduced in Windows Server 2003 R2 for the first time, DFS-R can help the administrator to overcome the limitations inherent to tapes and optical media.

DFS-R uses Remote Differential Compression (RDC), which only replicates changed parts of a file, which leads to a decrease in bytes transferred over the wire. Using such an efficient replication mechanism, DFS-R is an ideal solution to replicate branch office data into a central hub site for later long-term storage. In a recovery scenario, the data that needs to be restored will be replicated to the branch office.

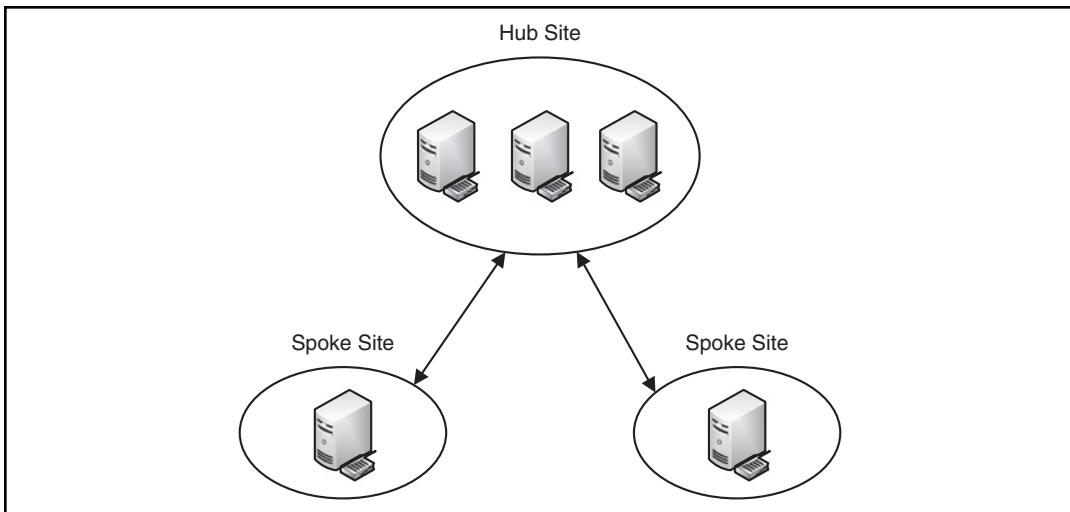
Another viable solution is System Center Data Protection Manager 2007 (SCDPM) from Microsoft. SCDPM is a pure backup product, providing continuous protection for most Microsoft application servers as well as file servers. Application servers include Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint Portal Server, and Microsoft Virtual Server.

SCDPM installs agents on protected systems to replicate data to a central backup server. Agents only replicate block level changes, therefore reducing the amount of bandwidth used. An intelligent filter technology reduces the amount of data needed for full backups and therefore reduces the time for the backup window. On the server side, Volume Shadow Copy technology creates snapshots of backed up data to enable disk-based recovery. SCDPM also has an interface for tape archiving.

Hub-and-Spoke Topology

Typically a branch office environment encompasses one or more hub sites and spokes sites that are connected to the hub or hubs (see Figure 6.1).

Figure 6.1 Hub-and-Spoke Topology



Hub sites can provide additional services for users in branch locations; that is, authentication and name resolution in case the local domain controller (DC) fails, centralized application access via terminal services (for example an ERP application), centralized e-mail services and backup facilities to name only a few. To avoid unnecessary network traffic between branch locations, branch office implementations often limit the connectivity between spoke sites by simply configuring a network router or, if not all but certain services should be limited, by modifying the service configuration.

What does modifying the service configuration mean? Here is an example: The network between your spoke sites is fully routed to access certain services between those sites. In case the local domain controller fails, clients should not authenticate to a domain controller in another spoke site—they should use domain controllers only in hub sites. To achieve this goal you would configure branch office domain controllers to register only site-specific records in DNS. Domain controllers from the hub site register DNS records for all sites—consequently, clients consider them as a backup. With this configuration, clients would authenticate to a local

domain controller only in their home site and fall back to domain controllers in the hub site, because domain controllers from other spoke sites have not registered to be available as backup.

Developing an Authentication Strategy

Seamless access to network resources is a big deal for most organizations. Different types of users, such as office workers, traveling employees, and perhaps customers or business partners need access to the network. At the same time, you need to maintain network security and information systems protection. Designing an authentication strategy means you find a balance between those two requirements.

Centralized Account Administration

A good starting point is a consolidated account database, such as Active Directory. By maintaining only one account database, you decrease administrative complexity. Administrators can create a single account for each user that allows the user to log on at different desktops, workstations, or notebooks in the domain by using the same username and a password or smart card. Without a centralized account management, different systems have to be maintained, secured, protected, and perhaps synchronized.

Single Sign-on

In an Active Directory based environment, users are required to enter a username and password or smart card only when first logging on. The validated user credentials are stored on the machine where the user logged on. Credential information then is used to authenticate the user to resources and applications in the same Active Directory forest and to other trusted forests.

A good example of a single sign-on application is Microsoft Exchange Server. Once the user logged in, Outlook can be started without the need to enter additional credentials to access the Mailbox on the Exchange Server. Instead, the logged on credentials are passed to the exchange server for authentication. Exchange server trusts the credentials because Exchange Servers are also members of Active Directory.

A password change will update the user account in Active Directory, replicate to all domain controllers in the same domain, and apply to all domain-joined systems.

To leverage single sign-on in heterogeneous environments, credentials need to be synchronized between different systems. Several tools exist to synchronize credential

information. Microsoft offers the Microsoft Identity Management (MIIS) Server for this kind of synchronization. This product recently has been renamed Identity Lifecycle Manager v2 (ILMv2). Apart from credential synchronization, ILM allows also for Smart Card enrollment. Windows Server 2008 also includes a password synchronization service for UNIX-based systems.

Kerberos Authentication

During domain logon, the client authenticates against a domain controller. Every domain controller in Active Directory acts as a Kerberos Key Distribution Center (KDC). The KDC running on a domain controller issues a ticket to the client to verify the user's identity. The ticket is stored in volatile memory and reused to authenticate the user to resources and applications running on other machines. Kerberos tickets are valid for a limited time (by default 10 hours) in which they are used to authenticate the user. After the ticket has expired, the client tries to renew the ticket for the user. This process occurs in the background and is fully transparent to the user.

NOTE

Kerberos uses a time stamp as an authenticator when issuing tickets. Hence, Kerberos authentication is highly dependent on functioning time synchronization. Without proper time synchronization, the user will not be able to log on, and access to resources will be denied. In an Active Directory network, all server and client computers automatically synchronize their time with a domain controller. Every domain controller in a domain synchronizes its time with the PDC Emulator of the domain and PDC Emulators synchronize their time with the PDC Emulator in a parent domain. On top of this chain is the PDC Emulator of the root domain, which should be synchronized with an external time source.

Password Policies

One of the new features of Windows Server 2008 Active Directory is the ability to create multiple password policies in a domain (also called *fine-grained password policies*). In the past, if you wanted to configure multiple password policies, you had to create multiple Active Directory domains or use third-party products, such as Specops Password Policy from Special Operations Software (<http://www.specopssoft.com>).

The ability to create multiple password policies also benefits branch office deployments. By using fine-grained password policies, you could assign a general password policy to all users (defined on the domain) and assign a special, stricter password policy to branch office administrators, therefore increasing security for those accounts. To use fine-grained password policies, all domain controllers must be running Windows Server 2008 and the domain must operate at the Windows Server 2008 domain functionality mode.

When to Place a DC in a Remote Office

If a domain controller is not available in the same location as the client, the client will try to log on at any domain controller that is registered in DNS as logon server for the client site. As mentioned earlier, in most implementations this will be a hub DC. In such a scenario, every part of the logon process is handled over the WAN link.

Influencing factors for the placement of a domain controller in a remote office are physical security, WAN link availability, user population, Active Directory aware applications, and Active Directory replication are some these factors. For example, a company might have strict requirements regarding the time it should take to log on. Logon time depends on the speed of the network link, the number of group policies that have to be processed, the number of logon scripts, and so on.

Number of Group Policies

When a client logs on, it queries the domain controller for its list of group policy and then downloads the GPOs to further apply them locally. The more policies the client needs to download and apply, the longer the logon takes. The use of folder redirection further increases the time.

Logon Scripts

Especially when you use a generic logon script to connect network drives for many different user groups, script processing can take a long time over a WAN link. In such a script, drive mappings are determined by group membership. At logon, a query is sent to the domain controller requesting group membership information for every user.

User Population

User population also influences logon performance. In branch office with few users, logon performance over a WAN link might be acceptable because the traffic generated to logon is minimal. In a location with many users, the WAN link might get congested very quickly, therefore affecting logon performance. This especially comes

into play when you have user populations with fixed working times, where all users log on at the same time in the morning.

Domain Controller Physical Security

As we mentioned before, physical security of server computers is often hard to ensure in a branch office. The recommendation is to not place a domain controller in a branch office where physical security cannot be guaranteed. A person who has physical access to a domain controller can attack the system by:

- Accessing disk information by booting an alternate operating system
- Removing physical disks
- Obtaining and/or manipulating a copy of a system state backup

You can address most of the weaknesses by using technology that is included in Windows Server 2008, such as BitLocker Drive Encryption and read-only domain controllers. Although it is important to remember that a solution that focuses only on the technology part can solve only part of the problem. More important is the definition of written policies and procedures that users must follow when managing domain controllers.

On-Site Technical Expertise Availability

Place domain controllers only in locations that include skilled personnel to manage the domain controller, or make sure domain controller management is possible remotely.

Authentication Availability

If your organization requires users to be authenticated at all times, you might consider placing a domain controller in a remote office where WAN link availability is not 100 percent.

WAN Link Speed and Bandwidth Utilization

Activities of a user or bandwidth shared by other systems or services might negatively affect WAN link performance. If the average bandwidth utilization affects logon performance for users, place a domain controller at that location.

Bandwidth and Network Traffic Considerations

Active Directory replication works differently depending on whether it is *intersite* or *intrasite* replication. DCs that are part of the same site (intrasite) replicate with one

another more often than DCs in different sites (intersite). If you have sites that are geographically dispersed, you need to be careful how you handle your GC server placement. The bandwidth between geographically dispersed offices is often minimal. The rule of thumb is to have GC servers in selected sites. In most cases, you do not want to have a GC server in every site because of the vast amount of replication that would occur. The following examples describe situations in which you should have a GC server within a site:

- If you have a slow WAN link between geographic locations. If you have a DC at each location, a good rule is also to have a GC server at each location. If the WAN link supports traffic for normal DC traffic, it should also handle GC traffic.
- If you have an application that relies heavily on GC queries across port 3268, you'll want to have a GC server in the site in which the application runs. An example of this is Exchange 2000, which relies heavily on GC information.
- You'll want to have GCs in as many sites as possible to support Universal Group membership authentication. We look at caching of Universal Groups, which can reduce traffic related to this, in the next section.

Data replicated between sites is compressed, which makes better use of available bandwidth. Because the data is compressed, more can be sent over a limited amount of bandwidth. This is how site placement and design can be critical to efficient network operation.

New & Noteworthy...

Microsoft Solution Accelerators for Design

To help you with the design of your infrastructure, Microsoft offers Solution accelerators. Solution accelerators provide flow charts to give you an overview of the planning process. They also describe the decisions that

Continued

have to be made and relate those decisions to the business requirements. Solution accelerators exist for all major technologies and are meant to augment the product documentation. They are available as a free download from Microsoft under <http://www.microsoft.com/downloads/details.aspx?FamilyId=AD3921FB-8224-4681-9064-075FDF042B0C&displaylang=en>.

Placing a Global Catalog Server in a Remote Office

Another consideration when it comes to replication is placement of your GC servers. In a small network with one physical location, GC server placement is easy. Your first DC that is configured will hold the GC role. If you have one site, but more than one DC, you can move the role to another DC if you want, or configure additional DCs as GCs. Most networks today consist of multiple physical locations, whether in the same city or across the country. If you have high-speed links connecting your branch offices you might be okay, but many branch office links use limited bandwidth connections. If the connection between locations is less than a T1, you might have limited bandwidth depending on what traffic is crossing the wire. As a network administrator, you will have to work with your provider to gauge how much utilization there is across your WAN links.

Another factor is reliability. If your WAN links are unreliable, replication traffic and synchronization traffic might not successfully cross the link. The less reliable the link, the more the need for setting up sites and site links between the locations.

Without proper planning, replication traffic can cause problems in a large network. Sites help to control replication traffic. Making the most of available bandwidth is an important factor in having a network that allows your users to be productive. Logon and searching Active Directory are both affected by GC server placement. If users cannot find the information they need from Active Directory, they might not be able to log on or find the information or data they need.

An often-underestimated factor is the use of Active Directory integrated applications such as Microsoft Exchange Server or Microsoft Office Live Communications Server. The placement of Exchange Servers directly impacts your domain controller placement. Microsoft Exchange Server 2003 and 2007 use Active

Directory Global Catalog Servers to look up recipient information. If you place an Exchange Server in your branch office without also placing a GC there, all recipient lookups would traverse the WAN link.

Universal Group Membership Caching

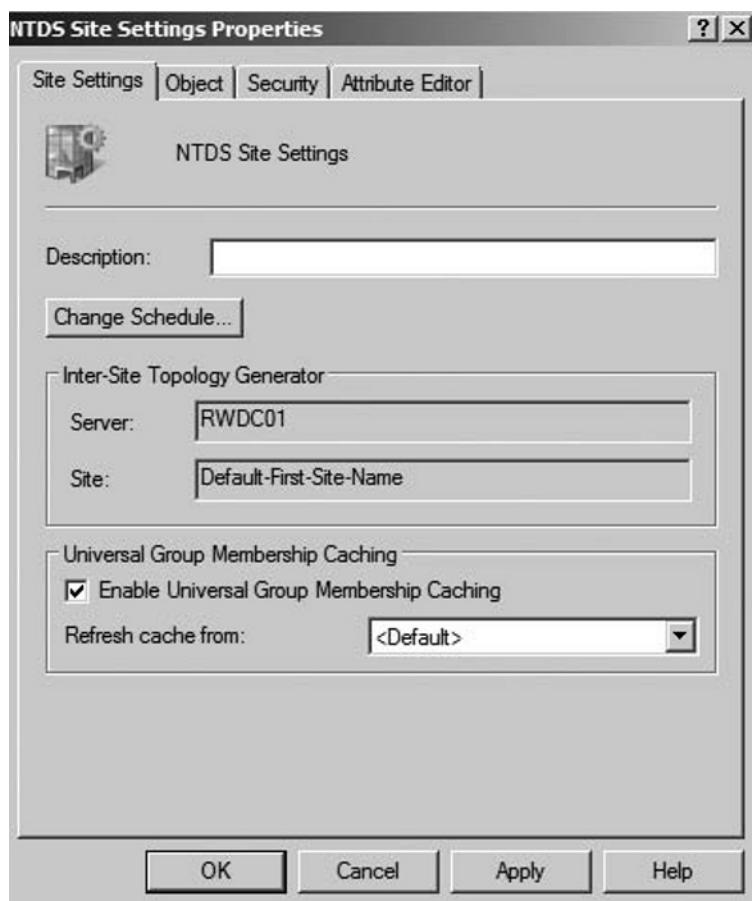
The Windows Server 2003 Active Directory introduced *Universal Group caching* as a new feature, and this feature is also available in Windows Server 2008. When a user logs on to the network, his or her membership in Universal Groups is verified. For this to happen, the authenticating DC has to query the GC. If the GC is across a WAN link, the logon process will be slow every time. To alleviate this, the DC that queries the GC can cache this information, which cuts down on the amount of data traveling across the WAN link for Universal Group information.

The cache is loaded at the first user logon. Every eight hours by default, the DC will refresh the cache from the nearest GC server. Caching functionality is administered in Active Directory Sites and Services, as shown in Figure 6.2, and can be turned off if desired. You can also designate the GC server from which you want the cache to refresh, giving you more control over traffic distribution on the network.

Prior to Windows Server 2003, Active Directory logon would immediately fail if a GC could not be located to check Universal Group membership. With Universal Group caching in Windows Server 2003 and Windows Server 2008, DCs cache complete group membership information, so even if a GC server cannot be reached, logon will still happen based on cached Universal Group information.

NOTE

The NTDS Site Settings Properties box is not the same NTDS Settings Properties box you accessed to make a DC act as a GC. Instead of accessing the properties of NTDS settings under the DC node in the Servers container, you must access the properties of NTDS site settings in the right console pane when you select a site name (e.g., Default-First-Site-Name). The similarity of these two settings can be confusing if you haven't worked with the console much.

Figure 6.2 Configuring Universal Group Caching

Full Domain Controller vs. Read-Only Domain Controller

You should install Full Domain Controllers in branch offices only if you have the need to write directly to the Active Directory database and if the application uses protocols such as DCOM or RPC to communicate with the DC. DCOM and RPC do not perform well over slow WAN links and should be used only on a local network. An example for an application that directly writes to Active Directory is Microsoft Exchange Server.

If there are no applications or services that write to Active Directory, an RODC is a better choice. RODCs have a read-only copy of Active Directory and therefore do not allow modifications to any object. Furthermore, RODCs do not replicate any user passwords unless defined by the administrator. Finally, role separation enables the administrator to assign local administrator rights to a domain user without granting any administrative rights for the domain or other domain controllers. We will cover RODCs in more detail later in this chapter.

Using BitLocker

Windows BitLocker is used to encrypt data on hard drives and volumes, and to validate the integrity of startup files. To provide this functionality, it makes use of a Trusted Platform Module (TPM). In case your computer is not equipped with a TPM, BitLocker can also be enabled for operation without it. The hardware and software requirements for BitLocker are:

- A computer that is capable of running Windows Server 2008
- A Trusted Platform Module version 1.2, enabled in BIOS
- A Trusted Computing Group (TCG)-compliant BIOS.
- Two NTFS disk partitions, one for the system volume and one for the operating system volume

Trusted Platform Modules

Developed by the Trusted Platform Group—an initiative by vendors such as AMD, Hewlett-Packard, IBM, Infineon, Intel, Microsoft, and others—a TPM is a semiconductor built into your computer motherboard. It is capable of generating cryptographic keys, limiting the use of those keys, and generating pseudo-random numbers.

Each TPM has a unique RSA key (the *endorsement key*) burnt into it that cannot be altered. The key is used for data encryption (a process known as *binding*). A TPM also provides facilities for *Secure I/O*, *Memory curtaining*, *Remote Attestation*, and *Sealed Storage*. You can secure your TPM module by assigning a TPM owner password.

With secure input and output (which is also known as *trusted path*), it is possible to establish a protected path between the computer user and the software that is

running. The protected path prevents the user from capturing or intercepting data sent from the user to the software process, for example playing a media file. The trusted path is implemented in both hardware (TPM) and software and uses checksums for the verification process.

Memory curtaining provides extended memory protection. With memory curtaining, even the operating system does not have full access to the protected memory area.

Remote attestation creates a hashed summary of the hardware and software configuration of a system. This allows changes to the computer to be detected.

Sealed storage protects private information in a manner that the information can be read only on a system with the same configuration. In the preceding example, sealed storage prevents the user from opening the file on a “foreign” media player or computer system. In conjunction, it even prevents the user from making a copy (*memory curtaining*) or capturing the data stream that is sent to the sound system (*secure I/O*).

A Practical Example

You download a music file from an online store. Digital rights management protects the file. All security methods are enforced: the file plays only in media players provided by the publisher (*remote attestation*). The file can be played only on your system (*sealed storage*) and it can neither be copied (*memory curtaining*) nor digitally recorded by the user during playback (*secure I/O*).

Introduction to BitLocker

Windows BitLocker ensures that operating system startup files are not modified and data on the disk is encrypted. By default BitLocker is configured to use a Trusted Platform Module (TPM) to ensure the integrity of the boot process at an early stage and to lock volumes that have been selected for BitLocker protection, making it very hard for intruders or thieves to get access to the computer. So even if the computer is tampered, the data is protected. If your computer system lacks TPM functionality, BitLocker allows you to configure USB sticks to store encryption keys. Although without a TPM, BitLocker can only encrypt the data on disk but cannot ensure the integrity of startup files.

The major features of BitLocker are full-volume encryption, checking the integrity of the startup process, recovery mechanisms, remote administration, and a process for securely decommissioning systems.

Full Volume Encryption

Windows BitLocker provides data encryption for volumes on your local hard drive. Unlike Encrypting File System (EFS), BitLocker encrypts all data on a volume—operating system, applications and their data, as well as page and hibernation files. In Windows Server 2008, you can use BitLocker to encrypt the whole *drive*, as compared to Windows Vista where you can encrypt *volumes*. BitLocker operation is transparent to the user and should have a minimal performance impact on well-designed systems. The TPM *endorsement key* is one of the major components in this scenario.

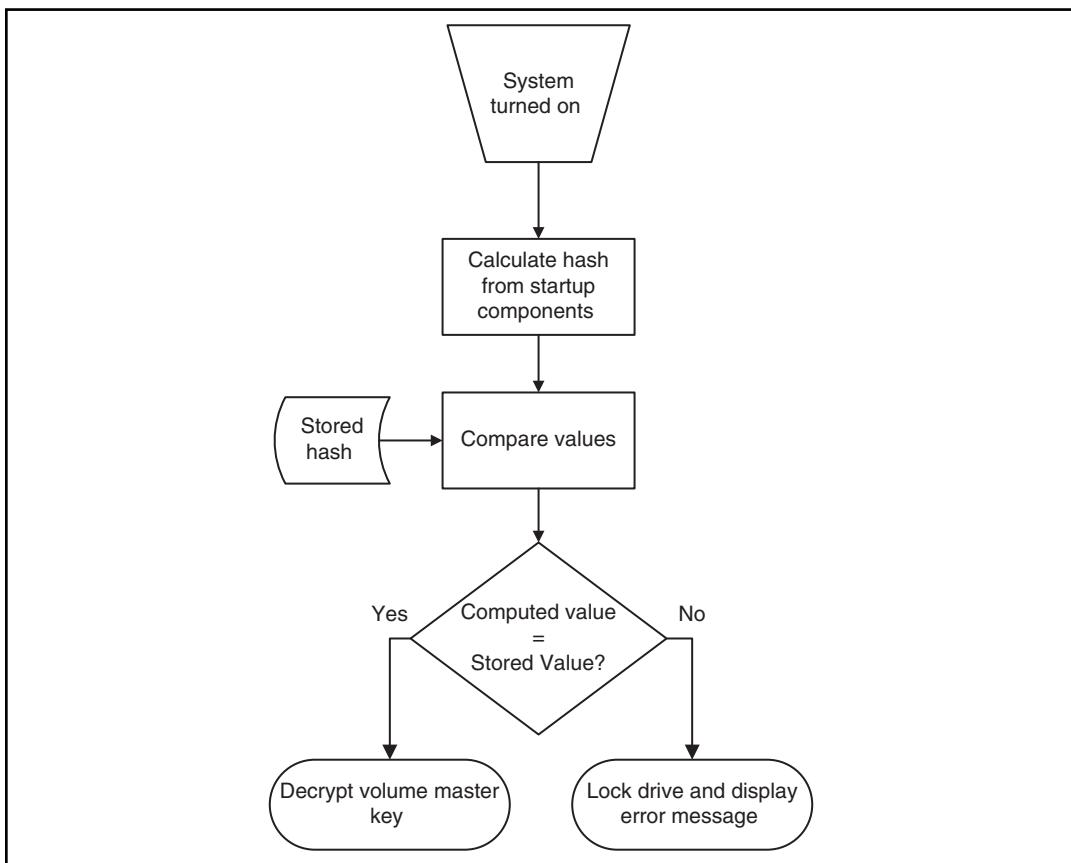
Startup Process Integrity Verification

Because Windows Startup components must be unencrypted for the computer to start, an attacker could gain access to these components, change the code, and then gain access to the computer, thereby gaining access to sensitive data such as BitLocker keys or user passwords as a consequence.

To prevent such attacks, BitLocker Integrity checking ensures that startup components (BIOS, Master Boot Record (MBR), boot sector, and boot manager code) have not been changed since the last boot.

Each startup component checks its code each time the computer starts, and calculates a hash value. This hash value is stored in the TPM and cannot be replaced until the next system restart. A combination of these values is also stored.

These values are also used to protect data. For this to work, the TPM creates a key that is bound to these values. The key is encrypted by the TPM (with the endorsement key) and can be decrypted only by the same TPM. During computer startup, the TPM compares the values that have been created by startup components with the values that existed when the key was created (see Figure 6.3). It decrypts the key only if these values match (see also *Sealed Storage*).

Figure 6.3 Startup Component Integrity Verification Flowchart

Recovery Mechanisms

BitLocker includes a comprehensive set of recovery options to make sure data not only is protected, but also available. When BitLocker is enabled, the user is asked for a recovery password. This password must be either printed out, saved to file on a local or network drive, or saved to a USB drive.

In an enterprise environment, however, you would not want to rely on each user to store and protect BitLocker keys. Therefore, you can configure BitLocker to store recovery information in Active Directory. We will cover key recovery using Active Directory later in this chapter.

Remote Administration

Especially in environments with branch offices, it is desirable to have a remote management interface for BitLocker. A WMI script provided by Microsoft allows for BitLocker remote administration and management. You will find the script in the **\Windows\System32** folder after you install BitLocker.

To manage a BitLocker protected system via script:

1. Logon as an administrator.
2. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. At the command prompt type **cd /d C:\Windows\System32**.
4. For example, to view the current status of BitLocker volumes, type **cscript manage-bde.wsf -status**.

Secure Decommissioning

If you decommission or reassign (maybe donate) equipment it might be necessary to delete all confidential data so that it cannot be reused by unauthorized people. Many processes and tools exist to remove confidential data from disk drives. Most of them are very time consuming, costly, or even destroy the hardware.

BitLocker volume encryption makes sure that data on a disk is never stored in a format that can be useful to an attacker, a thief, or even the new owner of the hardware. By destroying all copies of the encryption key it is possible to render the disk permanently inaccessible. The disk itself can then be reused.

There are two scenarios when deleting the encryption key:

- Deleting all key copies from volume metadata, while keeping an archive of it in a secure location such as a USB flash drive or Active Directory. This approach allows you to temporarily decommission hardware. It also enables you to safely transfer or ship a system without the risk of data exposure.
- Deleting all key copies from volume metadata without keeping any archive. Thus, no decryption key exists and the disk can no longer be decrypted.

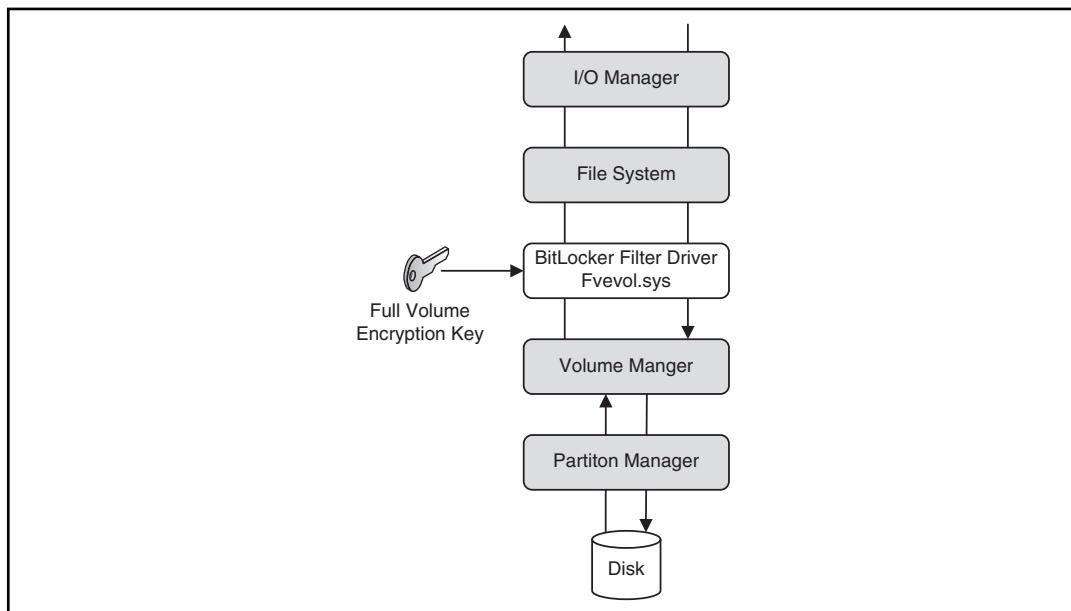
New & Noteworthy...

New Group Policy Settings to Support BitLocker

To support centralized administration of BitLocker, Group Policy (GPO) has been extended in Windows Server 2008 Active Directory. The new set of GPO settings allows for configuration of BitLocker as well as TPM. These can be found under Computer Configuration/Administrative Templates/Windows Components/BitLocker Drive Encryption and Computer Configuration/Administrative Templates/System/Trusted Platform Module. To configure these settings, make sure you have at least one Windows Vista or Windows Server 2008 Computer in your Active Directory to create a policy with the new settings available.

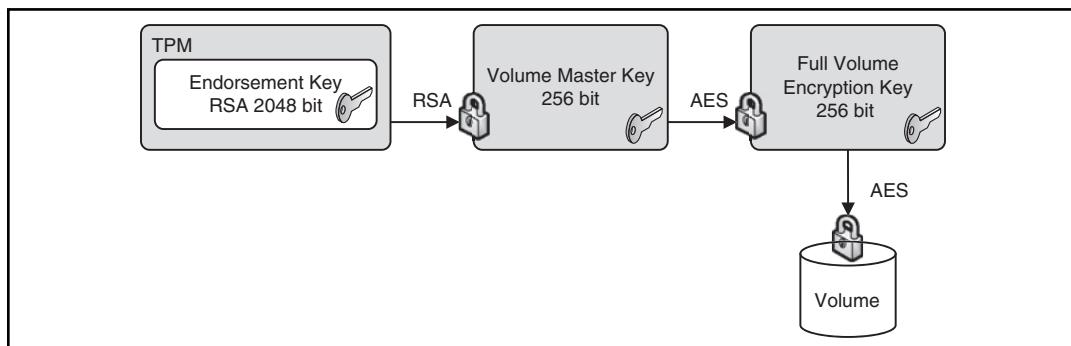
BitLocker Architecture

Once Integrity verification is successful, a filter driver encrypts and decrypts disk sectors transparently as data is written or read from the protected volume. The filter driver is a component of Windows Server 2008 or Vista and is inserted into the file system stack during BitLocker installation (see Figure 6.4), thus requiring a system restart. After the initial encryption of the volume is completed, BitLocker operation is completely transparent to the user.

Figure 6.4 Filter Driver Inserted into the File System Stack

Keys Used for Volume Encryption

Volume encryption does not simply create a single key, which it will use to encrypt the volume. In fact, a *full volume encryption key* is used to encrypt the entire volume. This key is a 256-bit Advanced Encryption Standard (AES) key. BitLocker encrypts the full volume key with a *volume master key*. The volume master key is also 256-bit AES. Finally, the volume master key is encrypted with the TPM *endorsement key*. As mentioned before, the endorsement key is a RSA key (see Figure 6.5).

Figure 6.5 Keys Used for Volume Encryption

Head of Class...

New Group Policy Settings to Support BitLocker

Why does BitLocker use a volume master key? Wouldn't it be easier to encrypt the full volume encryption key directly with the TPM endorsement key? At first glance, this would make sense. However, without the volume master key you would have to decrypt and reencrypt the entire volume in case an upstream key is lost or compromised.

Hardware Upgrades on BitLocker-Protected Systems

Thanks to the use of *volume master key*, upgrades of hardware such as CPU, motherboard, and such are not very time-consuming. To do so you have to disable BitLocker. Disabling BitLocker will *not* decrypt protected volumes. Instead, the volume master key will be encrypted with a symmetric key, which is stored unencrypted on the hard drive. Moving the disk to another BitLocker-enabled system and activating the volume is possible without any additional steps. Because the encryption key for the volume master key is stored unencrypted on the disk, administrators can boot the system and the reenable BitLocker.

By reenabling BitLocker the unencrypted key is removed from the disk, the volume master key is keyed and encrypted again, and BitLocker is turned back on.

BitLocker Authentication Modes

After Installation BitLocker can be configured to seamlessly integrate into the boot process (TPM only)—therefore being transparent to the user—or can require additional information in the form of a PIN or a startup key to initiate the boot process (TPM with PIN or startup key). The later scenarios add an additional layer of security through the use *multifactor authentication* options. TPM with PIN requires something the user *knows* (e.g., the PIN), TPM with startup key requires something the user *has* (e.g., a USB device).

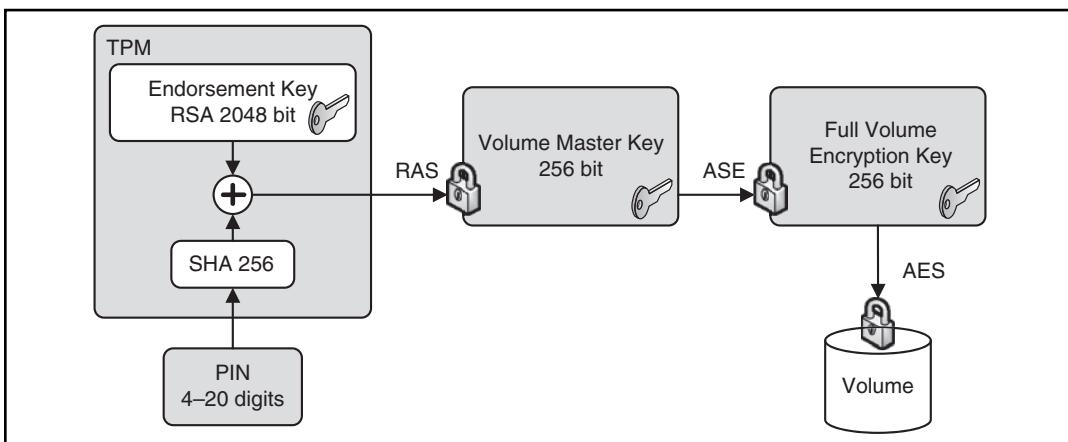
TPM Only

In this scenario, you enable BitLocker with a TPM only. No additional authentication options are used. BitLocker operation is completely transparent to the user and requires no interaction during the boot process.

TPM with PIN Authentication

Using TPM with PIN authentication, the administrator sets up a PIN during BitLocker initialization. The PIN is hashed using SHA-256 and the first 160 bits of the hash are used as authorization data for the TPM. The TPM uses the PIN data to seal the volume master key. Both the TPM and the PIN now protect the volume master key. During system startup or resume from hibernation, the user has to input the PIN to unseal the volume master key and initiate the boot process (see Figure 6.6).

Figure 6.6 Accessing a BitLocker-Enabled Disk That Is Secured with TPM + PIN



TPM with Startup Key Authentication

In this scenario the administrator creates a startup key during BitLocker initialization and stores it on any USB device that can be enumerated by the computer BIOS. During system startup or resume from hibernation, the user must insert the device. The device can be removed after the system has successfully booted.

Startup Key-Only

In this scenario, the administrator enables BitLocker on a computer without a TPM module. The startup key for the computer is generated during initialization and is stored on a USB flash drive. The computer user has to insert the USB flash drive each time the computer starts or resumes from hibernation.

A system configured to use a startup key-only configuration will not provide the same level of security as a system using one of the TPM modes. It will not check the integrity of system startup components. Using this scenario, make sure you create a Backup copy of the startup key! You do this by using the Control Panel BitLocker applet. The system saves the startup key with a .bek extension.

When to Use BitLocker on a Windows 2008 Server

In shared or unsecured environments such as branch offices, BitLocker can provide an additional level of security to a server. By securing the startup process and encrypting the operating system volume and all data volumes, BitLocker protects data from unauthorized access.

The BitLocker feature is not installed by default on Windows Server 2008. You would install it using Server Manager. Setup and maintenance are performed either by GUI tools or from the command line using a script, which also allows for remote management. On Windows Server 2008, BitLocker also integrates with Extensible Firmware Interface (EFI) computers to support IA64 hardware platforms. EFI is a newer, more flexible alternative to classical BIOS implementations. You should not install and enable BitLocker on a Windows Server 2008 Cluster machine, as it is a nonsupported scenario.

Encryption of data volumes on Windows Server 2008 is also supported. Data volumes are encrypted the same way as operating system volumes. Windows Server 2008 will automatically mount and decrypt these volumes on startup when configured to do so.

Support for Multifactor Authentication on Windows Server 2008

Multifactor authentication extends the security of BitLocker protected drives, although there are some constraints that you should think about when you plan to implement it.

PIN Authentication

Although it might not be desirable to use BitLocker with multifactor authentication on a Server, PIN authentication is a supported scenario on Windows Server 2008. If you manage a server remotely and have to reboot, who would enter the PIN? Of course, there are third-party solutions to overcome this limitation. Most of the modern server boxes offer a built-in remote management solution that is independent of the operating system. For example, Hewlett-Packard offers a so-called Integrated Lights Out (ILO) board to remotely connect to a server and transfer the screen to your desk.

If no remote management solutions were available, another possibility would be to instruct a trustworthy person at the branch office on how and when to enter the pin.

Startup Key Authentication

Of course, startup key support also is built into Windows Server 2008 BitLocker. All the facts mentioned for PIN support apply also to the startup key scenario, plus an additional one: startup keys protect the server only if the key is not left in the server after startup completes. Hence, there must be someone to insert and remove the USB device every time you reboot the server.

Enabling BitLocker

Due to its tight integration into the operating system, enabling BitLocker is straightforward. Before you begin installing and configuring, make sure that the machine you want to secure meets all software and hardware requirements. To enable BitLocker you must be a member of the local administrators group on your computer.

Partitioning Disks for BitLocker Usage

For BitLocker to work your system must have at least two partitions configured. The first, unencrypted partition is the system partition, which contains boot information. The second partition is the boot volume, which is encrypted and contains the operating system. Both partitions must be created before you install the operating system.

If you forgot to partition your system accordingly there's no way of reconfiguring your partitions (see Figure 6.7). Therefore, you must repartition your hard disk and reinstall the operating system from scratch.

Figure 6.7 BitLocker Refuses to Configure the System Due to an Invalid Partition Scheme



The drive configuration is unsuitable for BitLocker Drive Encryption. To use BitLocker, please re-partition your hard drive according to the BitLocker requirements.

Set up your hard disk for BitLocker Drive Encryption

NOTE

For Windows Vista Ultimate and Enterprise, Microsoft released the **BitLocker Drive Preparation Tool**. This Tool allows you to enable BitLocker even if you forgot to create the correct partitions before installation. It creates a partition, migrates the Windows boot files to the new partition, and finally activates the partition. To use the tool you need enough free disk space for the tool to operate. Unfortunately the tool is not available for Windows Server 2008.

EXERCISE 6.1

CREATING PARTITIONS FOR A BITLOCKER INSTALLATION

1. Start the computer from the Windows Server 2008 Product DVD.
2. In the Install Windows screen, choose your **Installation language**, **Time and currency format** and **Keyboard layout**, and then click **Next**.
3. In the **Install Windows** screen, click **Repair your Computer**.
4. In the **System Recovery Options** dialog box, make sure no operating system is selected. Then click **Next**.
5. In the **System Recovery Options** dialog box, click **Command Prompt**.
6. At the command prompt type **Diskpart** and then type **Enter**.
7. Type **select disk 0**.
8. Type **clean** to erase all existing partitions.
9. Type **create partition primary size=1500**. This will create a primary partition with a size of 1.5 GB.

10. Type **assign letter=B** to give this partition drive letter B.
 11. Type **activate** to set the partition as the active partition.
 12. Type **create partition primary** to create a partition with the remaining space. Windows Server 2008 will be installed on this partition.
 13. Type **assign letter=c**.
 14. Type **list volume** to see a display of all the volumes on this disk.
 15. Type **exit**.
 16. Type **format c: /y /f /fs:ntfs** to format the C volume.
 17. Type **format b: /y /f /fs:ntfs** to format the B volume.
 18. Type **exit**.
 19. Close the **System Recovery Options** window by clicking the close window icon in the upper right (do not click Shut Down or Restart).
 20. Click **Install now** to install Windows Server 2008. Use the larger partition for installation.
-

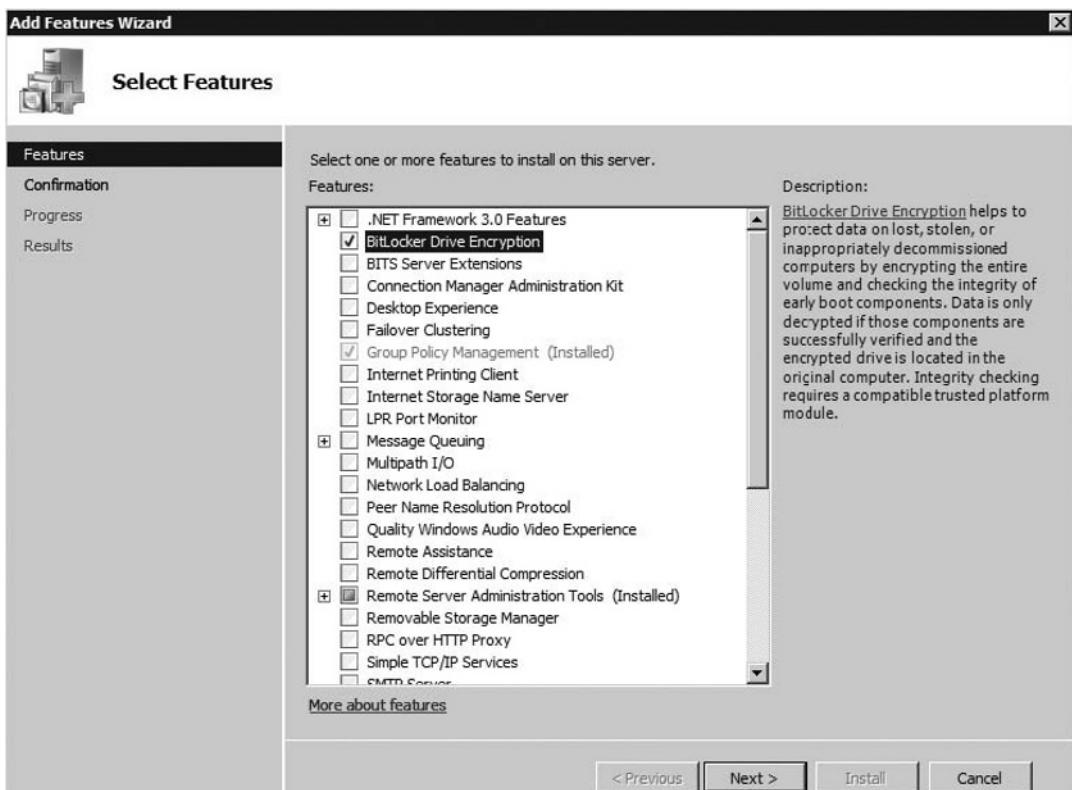
Installing the BitLocker on Windows Server 2008

As we already mentioned, BitLocker is a *Feature* of Windows Server 2008 and is not installed by default. To install BitLocker you use Server Manager as you would with all other roles and features. Be aware that a restart is required after installation. You can also install BitLocker from the command line by typing **ServerManagerCmd -install BitLocker-restart**.

EXERCISE 6.2

INSTALLING BITLOCKER

1. Logon as an administrator.
2. Click **Start | Administrative Tools | Server Manager**.
3. Scroll down to **Feature Summary**; click **Add Features**.
4. On the **Select Features** page, choose **BitLocker Drive Encryption** (see Figure 6.8), and then click **Next**.

Figure 6.8 Selecting the BitLocker Feature in Server Manager

5. On the **Confirm Installation Selections** page, click **Install**.
6. When installation is complete, click **Close**.
7. In the **Do you want to restart** window click **Yes**.

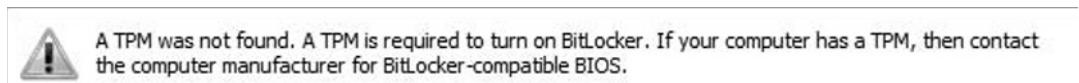
NOTE

Before you start with BitLocker configuration, make sure that you open Server Manager (in case you selected the **Do not show me this console at next logon** checkbox) and let the Post-Install wizard finish the installation.

Turning on BitLocker

After installing the BitLocker Feature on your Server and rebooting the system, you need to turn on BitLocker via a Control Panel applet. Make sure you are logged on as an administrator on the system and you have decided where to store the recovery password. In case your computer does not have a TPM module or the TPM module is not supported, you will receive a warning (see Figure 6.9).

Figure 6.9 Warning That a TPM Is Missing or Incompatible

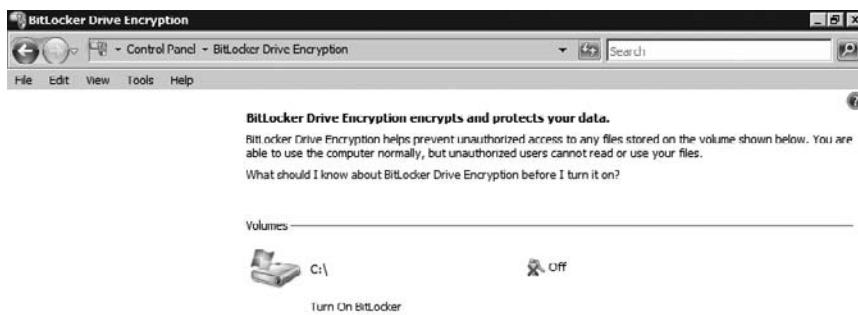


EXERCISE 6.3

TURNING ON BITLOCKER

1. Logon as an administrator.
2. Click **Start**, click **Control Panel**, and then click **BitLocker Drive Encryption**.
3. On the **BitLocker Drive Encryption** page, click **Turn On BitLocker** on the operating system volume (see Figure 6.10).

Figure 6.10 The Server Is Ready to Turn on BitLocker



See also

[Disk Management](#)

4. On the **BitLocker Drive Encryption Platform Check** dialog box click **Continue with BitLocker Drive Encryption**.
5. If your TPM is not initialized already, you will see the **Initialize TPM Security Hardware** screen.
6. On the **Save the recovery password** page, click **Save the password on a USB drive** (see Figure 6.11).

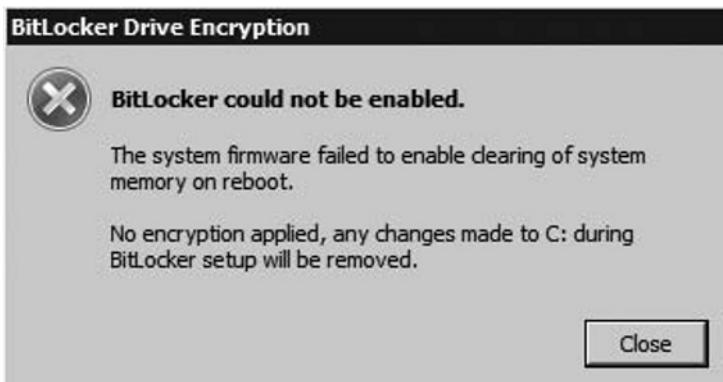
Figure 6.11 Saving the BitLocker Password



7. On the **Save a Recovery Password to a USB Drive** box, select your USB drive and click **Save**.
 8. On the **Encrypt the selected disk volume** page, confirm that the **Run BitLocker System Check** checkbox is selected, and then click **Continue**.
 9. Confirm that you want to reboot.
-

During the reboot phase, BitLocker verifies the system and makes sure it is ready for encryption. After rebooting the system, you should log back on to the system and verify that the **Encryption in Progress** status bar is displayed in the BitLocker Control Panel applet. In case your system cannot be enabled for BitLocker, an error message pops up during logon (see Figure 6.12).

Figure 6.12 Error Enabling BitLocker



TEST DAY TIP

If you do not have a TPM module in your computer or are using virtual machines, you will not be able to configure BitLocker as described in Exercise 6.3. Alternatively, you can continue with Exercise 6.5, which first enables BitLocker operation without a TPM and then continues with the configuration.

EXERCISE 6.4

TURNING ON BITLOCKER FOR DATA VOLUMES

1. Logon as an administrator.
2. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. At the command prompt type **manage-bde –on <volume>: -rp -rk F:**. This will encrypt the named volume, generate a recovery password, and store a recovery key on drive F:\ (which is the USB drive, in this example). Don't forget to record the recovery password!
4. At the command prompt type **manage-bde –autounlock –enable <volume>**: to enable automatic unlocking of the volume. The key to automatically unlock the volume on each restart is stored on the operating system volume, which must be fully encrypted before this command is issued.

NOTE

Windows Server 2008 mounts a protected data volume as normal. The keys for protecting a data volume are independent of the keys used to protect the operating system volume. The key-chain protecting the data volume is also stored on the encrypted boot volume, therefore allowing the boot volume to automatically mount any data volume after system restart.

Enable BitLocker Support for TPM-less Operation

The following steps configure your computer's Group Policy settings to turn on BitLocker on systems without a TPM.

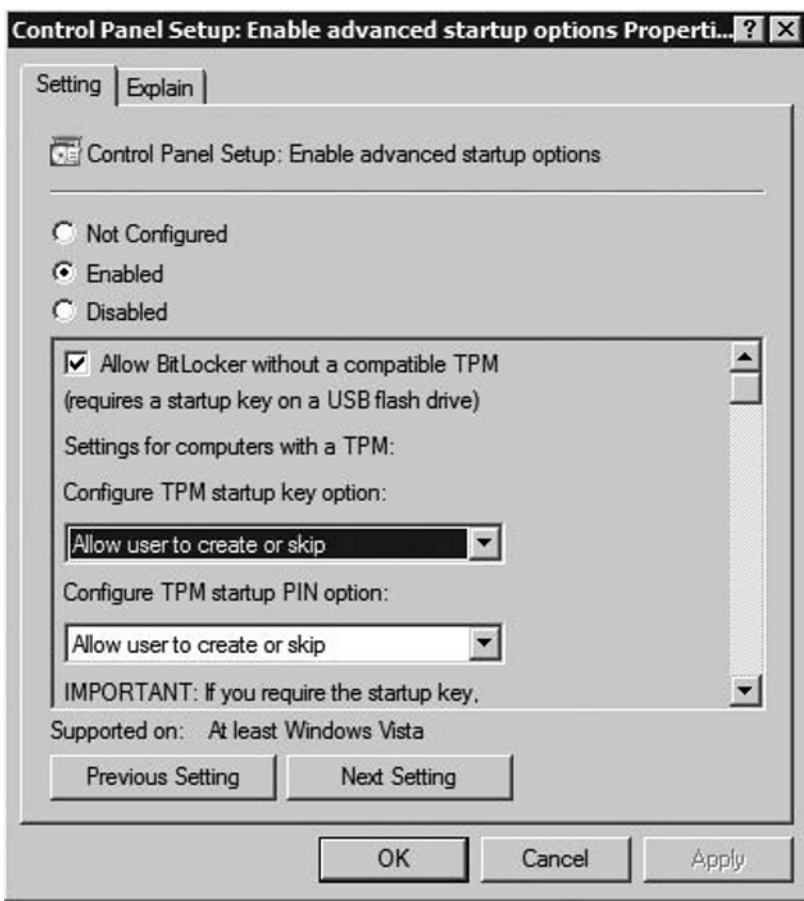
EXERCISE 6.5

CONFIGURING BITLOCKER FOR TPM-LESS OPERATION

1. Logon as an administrator.
2. Click **Start**, click **Run**, type **gpedit.msc** in the open box, and then click **OK**.

3. In the Local Group Policy Editor console tree, click **Local Computer Policy**, click **Administrative Templates**, click **Windows Components**, and then click **BitLocker Drive Encryption**.
4. Double-click the setting **Control Panel Setup: Enable Advanced Startup Options**.
5. Select the **Enabled** option, select the **Allow BitLocker without a compatible TPM** check box, and then click **OK** (see Figure 6.13).

Figure 6.13 Enabling TPM-Less Operation in the Local Group Policy



Turning on BitLocker on Systems without a TPM

Turning on BitLocker on systems without a TPM is similar to the normal activation process. Make sure you have a USB flash drive available to store the startup key.

EXERCISE 6.6

TURNING ON BITLOCKER ON SYSTEMS WITHOUT A TPM

1. Logon as an administrator.
2. Click **Start**, click **Control Panel**, and then click **BitLocker Drive Encryption**.
3. On the **BitLocker Drive Encryption** page, click **Turn On BitLocker** on the operating system volume.
4. On the **BitLocker Drive Encryption Platform Check** dialog box click **Continue with BitLocker Drive Encryption**.
5. On the **Set BitLocker startup preferences** page select **Require Startup USB key at every startup** (see Figure 6.14).

Figure 6.14 USB Startup Key Selection Screen



6. On the **Save your Startup Key** page select your USB drive from the list and click **Next**.
 7. On the **Save the recovery password** page, click **Save the password on a USB drive**.
 8. On the **Save a Recovery Password to a USB Drive** Box, select your USB drive and click **Save**.
 9. On the **Encrypt the selected disk volume** page, confirm that the **Run BitLocker System Check** checkbox is selected, and then click **Continue**.
 10. Confirm that you want to reboot.
-

Administration of BitLocker

In a managed Enterprise environment, it can be problematic to allow each user to enable BitLocker by themselves. Not only do you have to add the user to the local administrators group, you also give out the management of recovery passwords and/or PINs and startup keys. In the real world, users forget their passwords and PINs. So why should this be different with BitLocker recovery information? Here's an example: A user with a laptop decides to use BitLocker to make sure the data is secure even when the laptop is stolen. After enabling BitLocker, the user puts the recovery password printout into the laptop bag... A security nightmare!

One method to act upon such deficiencies is to educate users and increase their awareness so that they get more sensitive for security-related matters. Another approach might be technical. Windows Server 2008 extends well-known techniques and tools to give the administrator control over the BitLocker lifecycle. Group Policies settings were added to control the behavior of BitLocker on client and server systems. Furthermore, the Windows Management Instrumentation (WMI) Interface for BitLocker allows for local and remote management of BitLocker. We will talk about the possibilities of WMI later in this chapter.

Using Group Policy with BitLocker

Group Policy (GPO) in Windows Server 2008 has been extended to provide BitLocker specific configuration settings. With GPO, the administrator can control BitLocker installation and configuration as well as centralized storage of recovery passwords. Table 6.1 lists Windows Server 2008's Group Policy settings for BitLocker.

Table 6.1 Overview of Windows Server 2008 BitLocker Group Policy Settings

| Policy | Policy Path | Scope | Description |
|---|---|---------|--|
| Configure encryption method | Windows Components\BitLocker Drive Encryption | Machine | This policy setting allows you to configure the algorithm and key size used by BitLocker Drive Encryption. |
| Configure TPM platform validation profile | Windows Components\BitLocker Drive Encryption | Machine | This policy setting allows you to configure how the computer's Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if BitLocker has already been turned on with TPM protection. |
| Control Panel Setup: Configure recovery folder | Windows Components\BitLocker Drive Encryption | Machine | This policy setting allows you to specify the default path that is displayed when the BitLocker Drive Encryption setup wizard prompts the user to enter the location of a folder in which to save the recovery password. |
| Control Panel Setup: Configure recovery options | Windows Components\BitLocker Drive Encryption | Machine | This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to save BitLocker recovery options. |

Continued

Table 6.1 Continued. Overview of Windows Server 2008 BitLocker Group Policy Settings

| Policy | Policy Path | Scope | Description |
|--|---|---------|---|
| Control Panel Setup: Enable advanced startup options | Windows Components\BitLocker Drive Encryption | Machine | This policy setting allows you to configure whether the BitLocker Drive Encryption setup wizard will ask the user to set up an additional authentication that is requested each time the computer starts. You can further configure setting options for computers with and without a TPM. |
| Prevent memory overwrite on restart | Windows Components\BitLocker Drive Encryption | Machine | This policy setting controls computer restart performance at the risk of exposing BitLocker secrets. BitLocker secrets include key material used to encrypt data. |
| Turn on BitLocker backup to Active Directory Domain Services | Windows Components\BitLocker Drive Encryption | Machine | This policy setting allows you to manage the Active Directory Domain Services (AD DS) backup of BitLocker Drive Encryption recovery information. |

Storing BitLocker and TPM Recovery Information in Active Directory

In conjunction with Group Policy and a downloadable toolkit, Active Directory can be configured to store backup information for Windows BitLocker and the Trusted Platform Module. Recovery information includes the recovery password, the TPM owner password, and the information required to identify to which computers and volumes the recovery information applies. Optionally, you can also save a package

containing the actual keys used to encrypt the data as well as the recovery password required to access those keys.

As a best practice, configure Active Directory integration first and then allow BitLocker usage on clients and servers. If you enable BitLocker on clients first, recovery passwords for those computers are not stored in Active Directory, leading to an inconsistent experience in case you have to recover.

Storage of BitLocker Recovery Information in Active Directory

BitLocker recovery information is stored in Active Directory as a child object to the computer object. That is, the computer object acts as the parent container for a recovery object. Each BitLocker object includes the recovery password as well as other recovery information. Multiple recovery objects can exist under each computer account because there can be more than one recovery password for each protected volume.

BitLocker recovery information is stored in objects from type *msFVE-RecoveryInformation*. These objects are named after the following scheme:

<Object Creation Date and Time><Recovery GUID>

For example:

2008-01-30T08:17:05-09:00{063DC7a8-879D-DE34-FF6F-2417448D55CB}

Each msFVE-RecoveryInformation object contains the attributes listed in Table 6.2.

Table 6.2 Attributes Associated with the msFVE-RecoveryInformation Objects

| Attribute Name | Description |
|-------------------------|---|
| ms-FVE-RecoveryPassword | Contains the 48-digit recovery password |
| ms-FVE-RecoveryGuid | Contains the GUID associated with a BitLocker recovery password |
| ms-FVE-VolumeGuid | Contains the GUID associated with a BitLocker-supported disk volume |
| ms-FVE-KeyPackage | Contains a volume's BitLocker encryption key |

Storage of TPM Information in Active Directory

TPM owner passwords are stored as an attribute of the computer object in Active Directory. During TPM initialization or when the TPM password is changed, the hash of the password is stored in Active Directory in the *ms-TPM-OwnerInformation*.

Prerequisites

Since BitLocker Active Directory backup stores information in Active Directory objects, you need to extend the schema to support the storage of BitLocker-specific data. Schema extensions and scripts for enabling the Active Directory backup functionality are included in a downloadable toolkit from Microsoft. To access the download follow this link: <http://go.microsoft.com/fwlink/?LinkId=78953>. After extraction, the following sample scripts should help with the implementation:

- Add-TPMSelfWriteACE.vbs
- BitLockerTPMSchemaExtension.ldf
- List-ACES.vbs
- Get-TPMOwnerInfo.vbs
- Get-BitLockerRecoveryInfo.vbs

NOTE

BitLocker recovery information is stored in Active Directory attributes flagged as confidential. The confidential flag is a feature introduced in Windows Server 2003 Service Pack 1 and provides advanced access control for sensitive data. With this feature, only domain administrators and authorized users have read access to those attributes. Therefore Active Directory backup for BitLocker recovery information should be implemented only if your domain controllers are running Windows Server 2003 Service Pack 1, Windows Server 2003 R2, or Windows Server 2008, ensuring backed up BitLocker information is properly protected.

Extending the Schema

The first step in configuring Active Directory BitLocker backup is extending the Active Directory schema to allow storage of BitLocker specific objects (see Figure 6.15). Before you start, extract the toolkit files to a folder named **C:\BitLocker-AD**.

To extend the Active Directory schema:

1. Logon with an account that is a member of the schema admins group.
2. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. At the command prompt, type **cd /d C:\BitLocker-AD**.
4. At the command prompt, type **ldifde -i -v -f BitLockerTPMSchemaExtension.ldf -c "DC=X" "distinguished name of your domain" -k -j ..** Do not forget the period at the end of the command!

Figure 6.15 Schema Extension Output

```
C:\BitLocker-AD>ldifde -i -v -k -f BitLockerTPMSchemaExtension.ldf -c
"DC=X" "DC=nsoftincad,dc=internal" -j.

Connecting to "Alpha.Nsoftincad.Internal"
Logging in as current user using SSPI
Importing directory from file "BitLockerTPMSchemaExtension.ldf"
Loading entries

1: CN=ms-TPM-OwnerInformation,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry already exists, entry skipped

2: CN=ms-FVE-RecoveryGuid,CN=Schema,CN=Configuration,DC=nsoftincad,dc=internal
Entry already exists, entry skipped

3: CN=ms-FVE-RecoveryPassword,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry already exists, entry skipped

4: (null)
Entry modified successfully.

5: CN=ms-FVE-RecoveryInformation,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry already exists, entry skipped

6: CN=computer,CN=Schema,CN=Configuration,DC=nsoftincad,dc=internal
Entry modified successfully.
```

```
7: (null)
Entry modified successfully.

8: CN=ms-FVE-VolumeGuid,CN=Schema,CN=Configuration,DC=nsoftincad,dc=internal
Entry already exists, entry skipped

9: CN=ms-FVE-KeyPackage,CN=Schema,CN=Configuration,DC=nsoftincad,dc=internal
Entry already exists, entry skipped

10: (null)
Entry modified successfully.

11: CN=ms-FVE-RecoveryInformation,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

12: CN=ms-FVE-RecoveryInformation,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Attribute or value exists, entry skipped.

13: CN=ms-TPM-OwnerInformation,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

14: CN=ms-TPM-OwnerInformation,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

15: CN=ms-FVE-RecoveryGuid,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

16: CN=ms-FVE-RecoveryGuid,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

17: CN=ms-FVE-RecoveryGuid,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

18: CN=ms-FVE-RecoveryGuid,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

19: CN=ms-FVE-RecoveryPassword,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.

20: CN=ms-FVE-RecoveryPassword,CN=Schema,CN=Configuration,DC=nsoftincad,
dc=internal
Entry modified successfully.
```

```
21: CN=ms-FVE-RecoveryPassword,CN=Schema,CN=Configuration,DC=nsoftincad,  
dc=internal  
Entry modified successfully.  
22: (null)  
Entry modified successfully.  
15 entries modified successfully.  
The command has completed successfully
```

Setting Required Permissions for Backing Up TPM Passwords

The second step is to set permission in Active Directory. By default Windows Vista clients can back up BitLocker recovery information in Active Directory. However, to back up the TPM owner password an Access Control Entry (ACE) must be added to the computer object. To add the ACE use the **Add-TPMSelfWriteACE.vbs** script from the toolkit. To add the ACE entry:

1. Log on with a domain administrator account.
2. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. At the command prompt type **cscript Add-TPMSelfWriteACE.vbs**.

The script will add a single ACE to the top-level domain object in your domain. The ACE is inherited by all computer child objects in Active Directory.

Configuring Group Policy to Enable BitLocker and TPM Backup to Active Directory

The third step is to configure Group Policies for clients and servers to use BitLocker Active Directory Backup.

EXERCISE 6.7

ENABLING GROUP POLICY SETTINGS FOR BITLOCKER AND TPM ACTIVE DIRECTORY BACKUP

1. Logon with a domain administrator to any Domain Controller.
2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Group Policy Management**.

3. In the Group Policy Management Console, expand the forest tree down to the domain level.
 4. Right-click the **Default Domain Policy** and select **Edit**.
 5. In the Group Policy Management Editor, open **Computer Configuration**, open **Administrative Templates**, open **Windows Components**, and then open **BitLocker Drive Encryption**.
 6. In the right pane, double-click **Turn on BitLocker backup to Active Directory**.
 7. Select the **Enabled** option, select **Require BitLocker backup to AD DS**, and click **OK**. To further enable storage of TPM recovery information:
 8. Open **Computer Configuration**, open **Administrative Templates**, open **System**, and then open **Trusted Platform Module Services**.
 9. In the right pane, double-click **Turn on TPM backup to Active Directory**.
 10. Select the **Enabled** option, select **Require TPM backup to AD DS**, and click **OK**.
-



EXAM WARNING

In this example, we use the *Default Domain Policy* to configure Active Directory backup for BitLocker and TPM recovery information. However, in a real-world scenario you would create a new GPO that contains only BitLocker specific settings!

Recovering Data

BitLocker will lock the computer when an encryption key is not available. Likely causes for this can be:

- Inserting the BitLocker-protected drive into a new computer
- Replacing the computer motherboard
- Performing maintenance operation on the TPM (such as clearing or disabling)

- Updating the BIOS
- Upgrading critical early boot components that cause system integrity validation to fail
- Forgetting the PIN when PIN authentication has been enabled
- Losing the USB flash drive containing the startup key when startup key authentication has been enabled

When TPM fails to check the integrity of startup components, it will lock the computer at a very early stage before the operating system starts. When locked, the system enters recovery mode. You can use a USB flash drive with the recovery password stored on it or use the keyboard to enter the recovery password manually. In recovery mode, the keyboard assignment is somewhat different: you use functions keys to enter digits. F1 through F9 represents digits 1 through 9, F10 represents 0.

EXERCISE 6.8

TESTING BITLOCKER DATA RECOVERY

1. Logon as an administrator.
2. Click **Start**, click **Run**, type **tpm.msc** in the open box, and click **OK**. The **TPM Management Console** is displayed.
3. Under **Actions**, click **Turn TPM Off**.
4. Provide the TPM owner password, if required.
5. When the **Status** panel in the **TPM Management on Local Computer** task panel reads “Your TPM is off and ownership of the TPM has been taken,” close that task panel.
6. Click the **Safely Remove Hardware** icon in the notification area to remove the USB flash drive from the system.
7. **Restart** your computer. When you restart the computer, you will be prompted for the recovery password, because the startup configuration has changed since you encrypted the volume.
8. The **BitLocker Drive Encryption Recovery Console** should appear.
9. **Insert** your USB flash drive and press **ESC**. The computer will restart automatically.
10. The system should boot normally.



TEST DAY TIP

If you do not have a USB flash drive with the recovery password on it, you would press **ENTER** instead of **ESC**. After pressing **ENTER**, the system prompts you for the recovery password. Input the recovery password and press **ENTER** again.

Disabling BitLocker

If you want to turn off BitLocker, you need to decide if you want to disable BitLocker or decrypt the volume. Disabling BitLocker allows for TPM maintenance while the data is kept encrypted. Decrypting the volume means that the entire volume will be decrypted. Disabling BitLocker is supported only on operating system volumes and not on data volumes.

To turn off BitLocker Drive Encryption:

1. Click **Start**, click **Control Panel**, click **Security**, and then click **BitLocker Drive Encryption**.
2. On the **BitLocker Drive Encryption** page, find the volume on which you want BitLocker Drive Encryption turned off, and click **Turn Off BitLocker Drive Encryption**.
3. From the **What level of decryption do you want** dialog box, click either **Disable BitLocker Drive Encryption** or **Decrypt the volume** as needed.

Configuring Read-Only Domain Controllers

One of the biggest mistakes IT organizations make is underestimating the security risk presented by remote offices. As a consultant, I have seen many organizations (big and small) make major investments in their corporate IT security strategy, and then turn around and place a domain controller on top of a desk in a small/remote office—right next to an exit. Several times during the course of the day, employees, delivery people, solicitors, and others walk by this door—and often by the server itself. Typically, little exists to stop these people from walking out the door and selling their newly found (stolen) hardware on eBay. And this is probably

a best-case scenario. What would happen if the information on this server actually ended up in the wrong hands?

Read-only domain controllers were designed to combat this very problem. Remember: A domain controller stores all user passwords in its Active Directory database (although the passwords are hashed). This means that all the domain administrators' passwords also are stored! In a Windows 2000 Server or Windows Server 2003 Active Directory environment, placing such a domain controller in a remote office means that all passwords of all administrators in your domain are stored on a machine that might not be physically secured! Thanks to the newly introduced read-only domain controller things have changed.

Purpose

Based on the earlier information, the purpose of a read-only domain controller (RODC) is to provide authentication and authorization to users and computers in offices where physical security is hard to control. RODCs are one component in the Microsoft initiative to secure a branch office. Along with RODCs, you may also want to consider implementing BitLocker (whole-disk encryption), Server Core, as well as Role Separation—the ability to assign local administrator rights to an RODC without granting a user full domain administrator rights.

Features

RODC provides a number of features, which focus on providing heightened security without limiting functionality to the remote office users. Some of the key points here are:

- **Read-only replicas of the domain database.** Changes cannot be written directly to an RODC Active Directory database. RODC holds all the Active Directory Domain Services (AD DS) objects and attributes that a writable domain controller holds, with the exception of account passwords (credentials). Replication of passwords can be managed using password replication policies.
- **Support for Global Catalog role.** An RODC can also act as a Global Catalog Server.
- **Filtered Attribute Sets.** The ability to prevent certain AD attributes from being replicated to RODCs.

- **Unidirectional Replication.** Since changes cannot be written to an RODC Active Directory database, there is no need to replicate from an RODC to a full domain controller. This prevents potentially corrupt (or hijacked) data from being disbursed, and reduces unnecessary bandwidth usage.
- **Read-only DNS.** Allows one-way replication of application directory partitions, including ForestDNSZones and DomainDNSZones.
- **Credential caching.** Credential caching is the process of storing passwords for certain users or computers in the Active Directory database on an RODC, configured by an administrator. If an RODC is compromised, only the passwords of these accounts are stored in the active directory database. By default, no passwords are stored on the RODC. In case an RODC was stolen or hijacked, cached passwords can be reset and reports can be generated for auditing purposes.



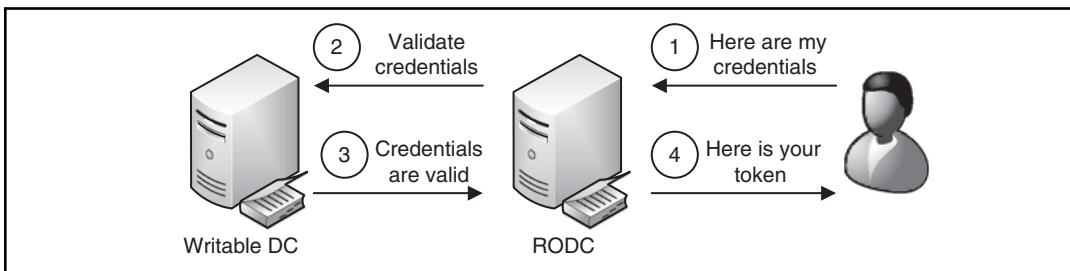
NOTE

RODCs are by no way a “reincarnation” of NT4 Backup Domain Controllers (BDC)!

Credential Caching

Credential caching is the process of storing passwords for user or computer accounts. As we mentioned earlier, by default no passwords are stored on an RODC except for its own computer account and a special Kerberos ticket account for that RODC. The administrator must explicitly allow caching of other credentials.

During authentication, an RODC will check its local Active Directory database to see if the account credentials are cached. In case credentials are cached, the account is authenticated locally. If credentials aren’t cached, the RODC contacts a writeable Windows Server 2008 domain controller in a hub site to validate the credentials and pass back the authenticated request (see Figure 6.16).

Figure 6.16 Credential Caching Explained

An RODC must always authenticate to a writeable domain controller in a direct connected site. Authentication chaining between RODCs is not supported!

Password Changes on an RODC?

To change a password, a client needs to contact a writable copy of Active Directory. If a user attempts to change the password, the client detects that the RODC is not writable and contacts a writable domain controller instead. If a password is changed on a writable Domain Controller, the RODC replicates only the changed password through a single-object-replication (RSO) request. However, the password is replicated again when the next replication cycle executes, because RSO operations do not trigger a unique sequence number update on the RODC.

In case a logon from a user with cached credentials fails, the RODC forwards the authentication request to a writable domain controller, which in turn forwards the request to the PDC emulator if required. If the authentication on the writable domain controller succeeds, the RODC will purge the locally stored password and replicate the new password by RSO operation.

RODCs and Kerberos Ticket Account

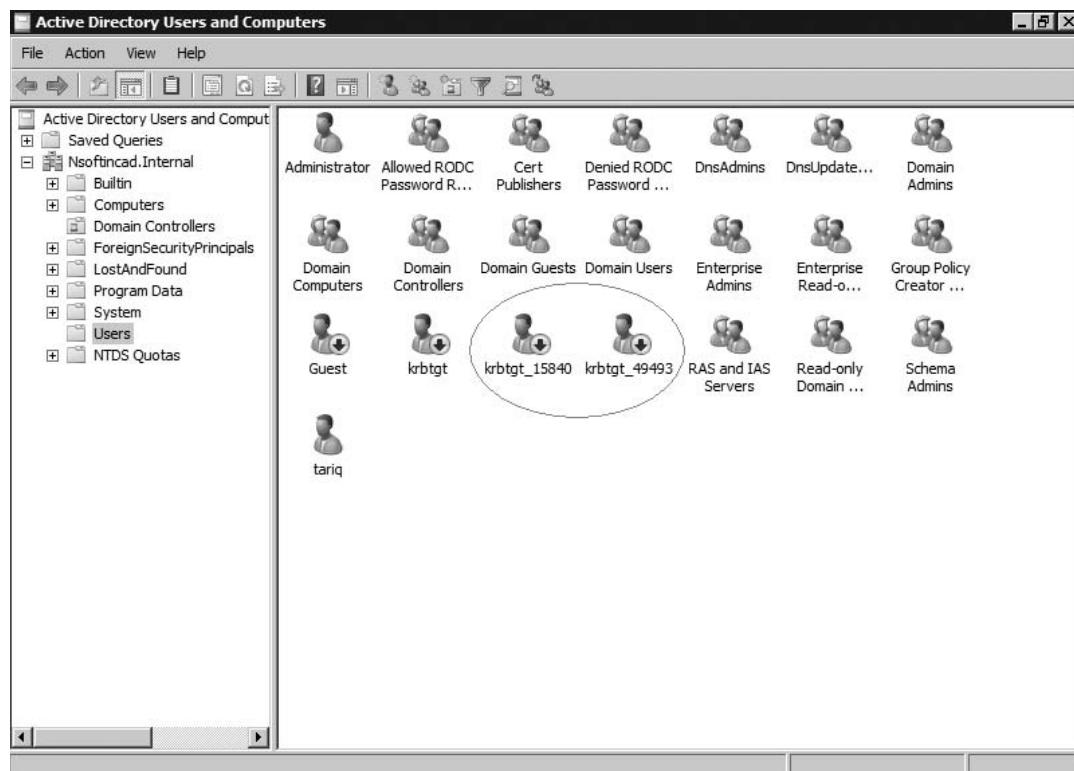
In an Active Directory Environment Kerberos is the primary mechanism used to authenticate accounts. Kerberos uses tickets to identify accounts and assign rights to them. Each domain controller is allowed to issue tickets and every ticket is digitally signed. To allow the signing of tickets with a key that is identical on every domain controller, a special user account exists in every domain: **krbtgt**.

This account signs all Kerberos tickets. It is the account with the strongest rights in the domain (see Figure 6.17). If this account is compromised, your Active Directory domain (and structure) is at risk. To mitigate this security risk in an

environment where RODCs are used, a special Kerberos ticket account is created for each RODC during domain controller promotion. It is named after the following convention: **krbtgt_randomnumber**.

This also allows for removal of a compromised RODC without interrupting or breaking authentication services for other branches or hub sites.

Figure 6.17 RODC krbtgt Accounts in Active Directory Users and Computers



NOTE

Krbtgt accounts are shown in Active Directory Users and Computers only if you enable the **Advanced Features** view. To enable it, click on **View** and select **Advanced Features**. All *krbtgt* accounts are created in the users container. Do not move or rename these accounts!

Read-Only Domain Name System

Most implementations of Active Directory I have seen as a consultant use Windows DNS Servers with Active Directory integrated DNS Zones. Advantages of such an implementation are:

- Replication of DNS data is managed by Active Directory
- Every DC has a writable copy of the DNS Zone (e.g., primary zone)
- Zone updates can be secured

Active Directory integrated DNS zones on a RODC are somewhat different.

On an RODC any data in Active Directory is read-only. In terms of DNS data, this means that an RODC hosts a newly introduced zone type: a *primary read-only Active Directory integrated zone*. This zone is created automatically when the DNS Server role is installed in an RODC. The writable copy of the data can be on any normal domain controller in Active Directory. Administrators of an RODC can view the DNS data stored in the primary read-only zone. However, modifications are possible only on a writable copy on a domain controller in the hub site. This also relates to role separation: a delegated administrator with local RODC administrator permissions cannot change any DNS data on an RODC.

Due to its read-only nature, DNS client updates are not processed on an RODC, since Name Server (NS) records for RODCs are not registered in DNS. When an RODC receives a DNS client update, it will return a referral to a writable copy of the DNS zone (similar as with a standard primary–standard secondary scenario). The client will then attempt the update on the DNS server provided in the referral. Once the data has changed on the writable copy, the RODC replicates only this updated DNS record in a RSO request.

Installing an RODC

RODCs work well in existing Active Directory environments. The requirements to install an RODC in an existing Active Directory are Windows Server 2003 Forest Functionality Level and at least one Windows Server 2008 domain controller (no RODC), which must hold the Primary domain controller (PDC) Emulator flexible single master operations (FSMO) role. There is no need to upgrade down-level domain controllers. Windows Server 2003 Forest Functional Level is required so that linked-value replication and Kerberos constrained delegation is available.

A Full Window Server 2008 domain controller is needed, because the RODC must forward authentication request for accounts for which the passwords are not

stored on the RODC. In addition, this domain controller checks if the password should be replicated to the RODC. Finally, the need for the PDC Emulator role has to do with the special Kerberos Ticket Account used by RODCs. Accounts of this type can be created only on a domain controller that owns the PDC Emulator role.

Head of the Class...

Adding an RODC to an Existing Forest

If you install an RODC into an existing forest, make sure you first prepare the Active Directory forest for the addition of an RODC. This is done by using the tool **adprep**, which can be found on the Windows Server 2008 DVD in the folder **\sources\adprep**. You may have used this tool to upgrade your Active Directory schema and to prepare a domain in the past. Execute the tool on the domain controller that holds the Infrastructure Master FSMO role. To prepare Active Directory for RODC operations, log on with an Enterprise Admin account and run **adprep /rodcprep**. This will add permissions on all DNS application partitions in Active Directory. Before you continue with the RODC installation, make sure that the changes have been replicated throughout the entire forest.

EXERCISE 6.9

VERIFYING RODC INSTALLATION PREREQUISITES

1. Log on as an Enterprise Admin of the forest you are checking.
2. Click on **Start | Administrative Tools | Active Directory Domains and Trusts**.
3. Right-click the **Active Directory Domains and Trusts** node and select **Raise Forest Functional Level**.
4. In the Raise forest functional level dialog make sure the Forest functional level is Windows Server 2003. The Forest functional level appears under **Current Forest Functional Level**.

Installation of an RODC

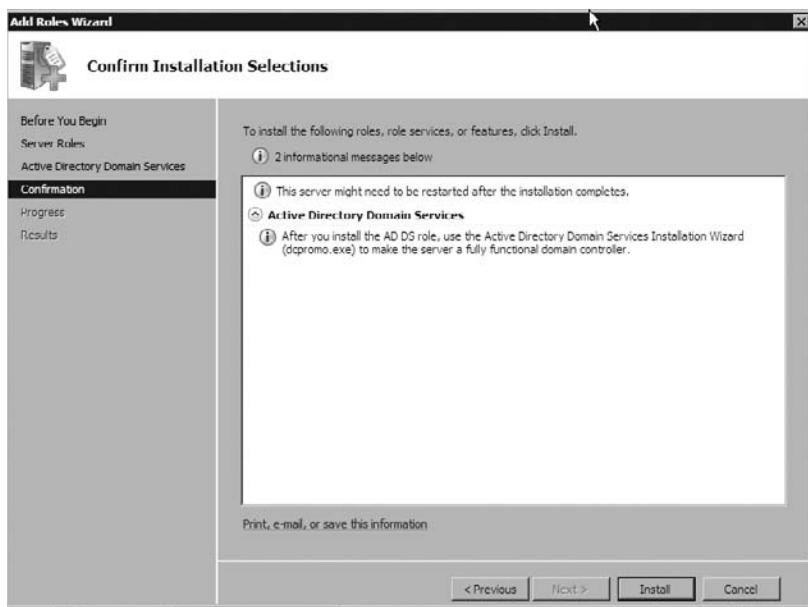
Installing an RODC doesn't have many differences to the installation process of a normal DC. You also use DCPROMO to promote a member server to an RODC. The only difference is that you have to select a single checkbox to designate that the wizard should promote an RODC instead of a normal DC.

EXERCISE 6.10

INSTALLING AN RODC

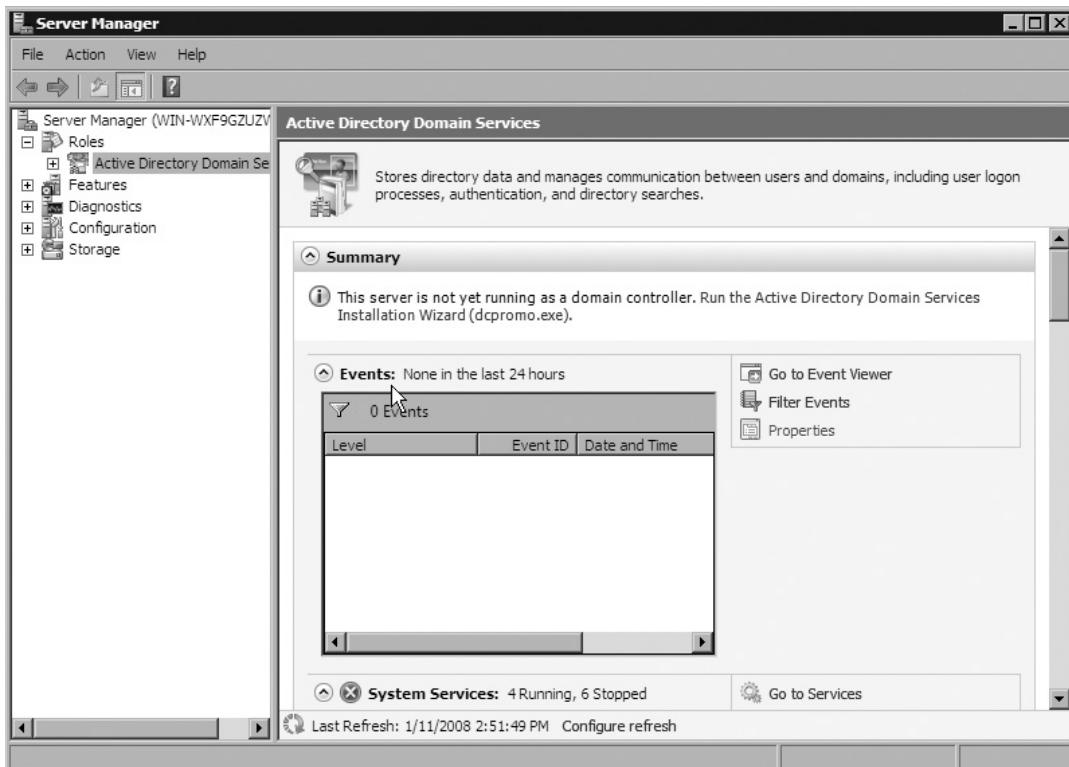
1. Log on as a local administrator on the server your are installing.
2. Click **Start | Administrative Tools | Server Manager**.
3. Scroll down to **Role Summary**, click **Add roles**.
4. When the **Before You Begin** page opens, click **Next**.
5. On the **Select Server Roles** page, choose **Active Directory Domain Services**, and then click **Next**.
6. Click **Next** again on the **Active Directory Domain Services** page.
7. On the **Confirm Installation Selections** page (see Figure 6.18), click **Install**.

Figure 6.18 Confirming Installation Selections



8. When installation is complete, click **Close**.
9. If the Server Manager window has closed, re-open it.
10. Expand **Roles**, and then click **Active Directory Domain Services**.
11. Under Summary (see Figure 6.19), click the link to **Run The Active Directory Domain Services Installation Wizard**.

Figure 6.19 Active Directory Domain Services Summary Page in Server Manager



12. Click **Next** on the **Welcome To The Active Directory Domain Services Installation Wizard** page.
13. On the **Operating System Compatibility** page, click **Next**.
14. On the **Choose a Deployment Configuration** page, click **Existing Forest**.
15. Ensure **Add a Domain Controller to an Existing Domain** is selected, and then click **Next**.

16. On the **Network Credentials** page, type the name of your domain and click **Set**.
 17. In the **User Name** field, type <domain>\administrator.
 18. In the **Password** field, type your administrator password, and then click **OK**.
 19. Click **Next**.
 20. On the **Select a Domain** page, click **Next**.
 21. On the **Select a Site** page (if you have Sites and Services configured), you can choose to which site to add this RODC. In this case, we are using the default site; click **Next**.
 22. Select **DNS Server** and **Read-Only Domain Controller** on the **Additional Domain Controller Options** page and then click **Next**.
 23. In the **Group Or User** field, type <domain>\administrator, and then click **Next**.
 24. Verify the file locations, and click **Next**.
 25. On the **Active Directory Domain Services Restore Mode Administrator Password** page, type and confirm a restore mode password, and then click **Next**.
 26. On the **Summary** page, click **Next**.
 27. The Active Directory Domain Services Installation Wizard dialog box appears. After installation, reboot the server.
-



TEST DAY TIP

When you install a domain controller, it is possible to skip the installation of the Active Directory Domain Services (AD DS) role. Instead, you run DCPROMO directly from **Start | Run**. DCPROMO will copy AD DS binaries if necessary. After the binaries have been copied to the system (which is equal to running the AD DS role installation), DCPROMO will pop up and promotion continues as mentioned in the exercise. Caution: This procedure is valid only for the AD DS role!

Configuring & Implementing...

Installing RODC from Media

RODCs can also be installed from media. To use the Install from Media feature during DCPROMO, you first have to create an Installation Media from which DCPROMO can extract the data. The process for creating an Installation Media has changed in Windows Server 2008. In Windows Server 2003 (the Version in which Install from Media was introduced) you have to back up the system state of a domain controller and then restore the backup to an alternate location. In Windows Server 2008, you create an Install Media with NTDSUTIL. To use the Install Media with DCPROMO you simply select the checkbox **Use Advanced Mode Installation** on the first wizard page.

Prestaging RODC Computer Accounts

Normally only members of the Domain Admins group are allowed to install a domain controller. With Windows Server 2008 and RODCs, Microsoft added the ability to delegate the installation of an RODC. In order to do this, a domain admin must prestage an RODC computer account in Active Directory Users and Computers. In the prestaging wizard (which is a special appearance of the DCPROMO wizard), you define the name of the RODC and on the **Delegation of RODC Installation and Administration** page you select a user group who is permitted to complete the RODC installation after the account has been created.

During final installation of a prestaged RODC, DCPROMO will automatically detect (based on the computer name) the existing RODC object and attach the physical machine to the existing account in Active Directory. It is also possible to complete the installation from the command line by specifying the following command: **dcpromo /UseExistingAccount: Attach**.

EXAM WARNING

Please keep in mind that the name of the prestaged RODC must be unique in Active Directory! This means if you already have a computer object in Active Directory with the same name as the RODC, DCPROMO refuses to create the RODC object.

EXERCISE 6.11

PRESTAGING AN RODC COMPUTER ACCOUNT

For this exercise, you need a user account with no administrator rights. In our example, we will use a user account Nsoftincad\Tariq to delegate the RODC installation.

1. Logon as a domain admin of the domain to which you are adding an RODC.
2. Click **Start | Administrative Tools | Active Directory Users and Computers**.
3. In Active Directory Users and Computers right-click the **Domain Controllers** organizational unit and select **Pre-create Read-only Domain Controller account....**
4. Click **Next** on the **Welcome To The Active Directory Domain Services Installation Wizard** page.
5. On the **Operating System Compatibility** page, click **Next**.
6. On the **Network Credentials** page, make sure that **My current logged on credentials** is selected, and click **Next**.
7. On the **Specify a Computer Name** page, type the name of the RODC computer and click **Next**.
8. On the **Select a Site** page (if you have Sites and Services configured), you can choose to which site to add this RODC. In this case, we are using the default site; click **Next**.
9. Select **DNS Server** and **Read-Only Domain Controller** on the **Additional Domain Controller Options** page and then click **Next**.
10. In the **Group Or User** field, type **Nsoftincad\Tariq**, and then click **Next**.
11. On the **Summary** page, click **Next**.
12. The Active Directory Domain Services Installation Wizard dialog box appears for a few seconds and then exits. No reboot is required at this stage!

NOTE

After the wizard finishes the creation of the RODC account, you will see a new domain controller computer object in the **Domain Controllers OU** in **Active Directory Users and Computers**. Until the RODC installation is finished, this computer object is *unoccupied*, meaning the account is disabled and only a physical computer with the same name can be attached.

TEST DAY TIP

During the process of prestaging an RODC account, it is also possible to specify advanced parameters for the account creation. You do this by selecting the checkbox **Use advanced Mode Installation**. The advanced mode installation allows you to modify the default Password Replication Policy. Furthermore, it allows you to select an Install Media for the RODC installation.

EXERCISE 6.12**COMPLETING THE INSTALLATION OF A PRESTAGED RODC**

In Exercise 6.11 we prestaged an RODC computer account. In this exercise, we will complete the installation on the RODC machine itself using the delegated user account **Nsoftincad\Tariq**.

1. Logon as a local administrator on the server you are installing.
2. Click **Start**, click **Run**, type **DCPROMO** in the open box, and click **OK**.
3. Click **Next** on the **Welcome To The Active Directory Domain Services Installation Wizard** page.

4. On the **Operating System Compatibility** page, click **Next**.
 5. On the **Choose A Deployment Configuration** page, click **Existing Forest**.
 6. Ensure **Add A Domain Controller To An Existing Domain** is selected, and then click **Next**.
 7. On the **Network Credentials** page, type the name of your domain and click **Set**.
 8. In the **User Name** field, type **Nsoftincad\Tariq**.
 9. In the **Password** field, type your administrator password, and then click **OK** (see Figure 1.10).
 10. Click **Next**.
 11. On the **Select a Domain** page, click **Next**.
 12. On the **Active Directory Domain Services Installation Wizard** dialog click **Yes**.
 13. On the **Active Directory Domain Services Installation Wizard** dialog click **Next**.
 14. Verify the file locations, and click **Next**.
 15. On the **Active Directory Domain Services Restore Mode Administrator Password** page, type and confirm a restore mode password, and then click **Next**.
 16. On the **Summary** page, click **Next**.
 17. The Active Directory Domain Services Installation Wizard dialog box appears. After installation, reboot the server.
-



TEST DAY TIP

As an alternative, you could also use the command **dcpromo /UseExistingAccount: Attach** to complete the installation.

Full Server Installation vs. Server Core Installation

In Terms of Security, Server Core is a perfect foundation for an RODC. Due to its lack of the Windows shell (e.g., explorer.exe, Internet Explorer, etc.) and its cut-down

roles and features, it has a smaller footprint and, more important, a smaller attack surface. A smaller attack surface means less vulnerability and therefore less patching.

Also so-called social engineering on a Server Core machine might not be as attractive as on a normal system. Can you imagine an employee logging on to a server core machine and all that comes up is a command prompt? Without knowing the right commands, it would be a very frustrating experience.

Installing an RODC on Server Core is straightforward. There are only a few differences to a normal server system:

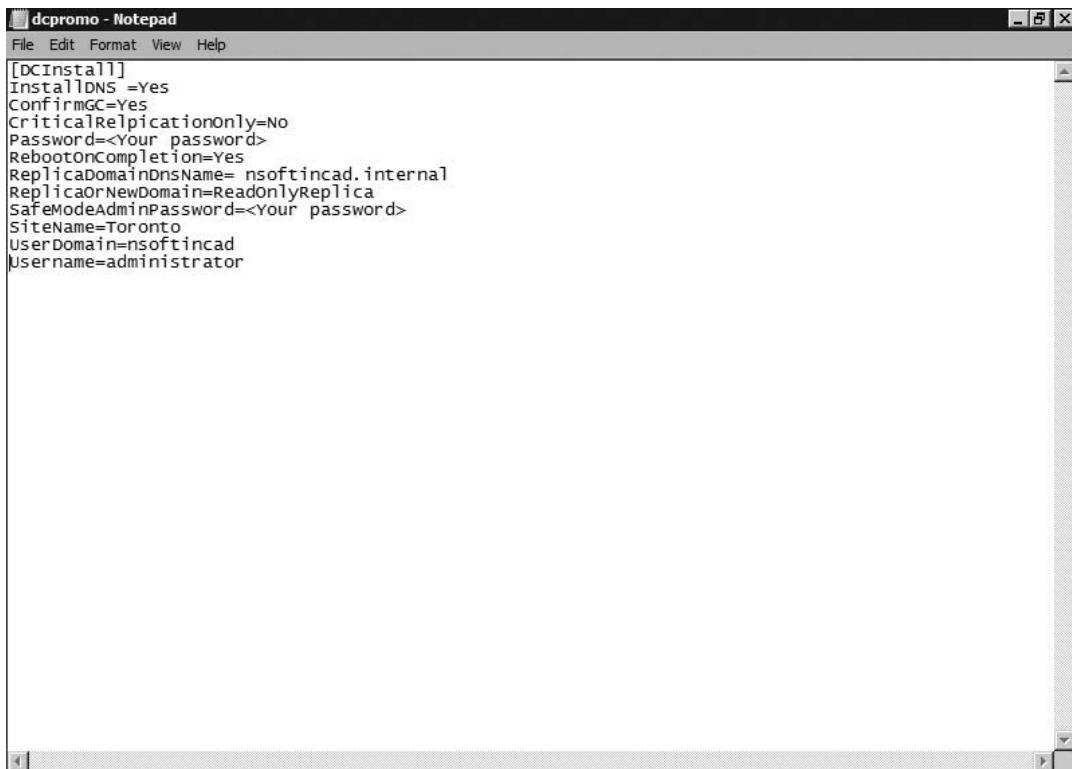
- You must not install the AD DS role before running DCPROMO (it does this for you).
- You need to create an unattended installation file or provide command line switches to DCPROMO when you start the installation process.

EXERCISE 6.13

INSTALLING AN RODC ON SERVER CORE

In this exercise, you will install an RODC on a Server Core machine. To automate the installation you will prepare an answer file that you use later on with DCPROMO.

1. Log on as a local administrator on the server you are installing.
2. At the command prompt type **Notepad** and press **Enter**.
3. Create an answer file. An example is shown in Figure 6.20.

Figure 6.20 DCPROMO Answer File for Installation on Server Core

4. In Notepad click **File | Save** and save the file with a filename of **dcpromo.txt**.
5. **Close** Notepad.
6. At the command prompt type **dcpromo /answer:dcpromo.txt**. After DCpromo finishes, the system will automatically reboot. Figure 6.21 shows the DCpromo output during installation on Server Core.

Figure 6.21 DCpromo Output during Installation on Server Core

```
C:\Users\administrator>dcpromo /answer:dcpromo
Checking if Active Directory Domain Services binaries are installed...
Active Directory Domain Services Setup
Validating environment and parameters...
```

The following actions will be performed:

Configure this server as an additional Active Directory domain controller for the domain nsoftincad.Internal.

Site: Default-First-Site-Name

Additional Options:

Read-only domain controller: Yes

Global catalog: Yes

DNS Server: Yes

Update DNS Delegation: No

Source domain controller: any writable domain controller

Password Replication Policy:

Allow: NSOFTINCAD\Allowed RODC Password Replication Group

Deny: BUILTIN\Administrators

Deny: BUILTIN\Server Operators

Deny: BUILTIN\Backup Operators

Deny: BUILTIN\Account Operators

Deny: NSOFTINCAD\Denied RODC Password Replication Group

Database folder: C:\Windows\NTDS

Log file folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

The DNS Server service will be installed on this computer.

The DNS Server service will be configured on this computer.

This computer will be configured to use this DNS server as its preferred DNS server.

Starting...

Performing DNS installation...

Press CTRL-C to: Cancel

Waiting for DNS installation to finish

..

Waiting for DNS Server service to be recognized... 0

Waiting for DNS Server service to start... 0

Checking if Group Policy Management Console needs to be installed...

Changing domain membership of this computer...

Located domain controller Alpha.Nsoftincad.Internal for domain Nsoftincad.Internal

Stopping service NETLOGON

Configuring the local computer to host Active Directory Domain Services

```
Replicating the schema directory partition  
Replicating CN=Schema,CN=Configuration,DC=Nsoftincad,DC=Internal: received  
1069 out of approximately 1558 objects  
Replicating CN=Configuration,DC=Nsoftincad,DC=Internal: received 1069 out of  
approximately 4085 objects  
Replicating secrets for Read-only Domain Controller.  
Setting the computer's DNS computer name root to Nsoftincad.Internal  
Securing machine\software\microsoft\windows  
Securing machine\system\currentcontrolset\control  
Replicating the domain directory partition...  
Press CTRL-C to: Finish Replication Later  
Replicating DC=ForestDnsZones,DC=Nsoftincad,DC=Internal: received 19 out of  
approximately 19 objects  
The attempted domain controller operation has completed  
Configuring the DNS Server service on this computer...  
Active Directory Domain Services is now installed on this computer for the  
domain Nsoftincad.Internal.  
This Active Directory domain controller is assigned to the site  
Default-First-Site-Name. You can manage sites with the Active Directory Sites  
and Services administrative tool.  
You must restart this computer to complete the operation.
```

Configuring an RODC

Password Replication Policies are the basis for credential caching. Stored in Active Directory on the Computer Object of each RODC, a Password Replication Policy is a list of accounts for which the password is permitted or denied from being cached. An administrator may change the list of permitted or denied accounts by modifying the Password Replication Policy in Active Directory Users and Computers.

When a writeable Windows Server 2008 domain controller receives an authentication request from an RODC, it checks the RODC's Password Replication Policy to determine if the credentials of the account should be replicated to the RODC. In case the Password Replication Policy permits replication of the credentials, RODC will replicate and store them locally. Subsequent logons by the same account can then be serviced directly by the RODC without contacting a writable domain controller.

A Password Replication Policy contains several entries, from which only one is set to Allow by default (see Table 6.3).

Table 6.3 Default Password Replication Policy Settings

| Entry | Setting |
|---|----------------|
| Account Operators | Deny |
| Administrators | Deny |
| Allowed RODC Password Replication Group | Allow |
| Backup Operators | Deny |
| Denied RODC Password Replication Group | Deny |
| Server Operators | Deny |

To support RODC operations, Microsoft has introduced two new built-in Domain Local Groups in Windows Server 2008 Active Directory. Both can be found in the *Users* Container in Active Directory:

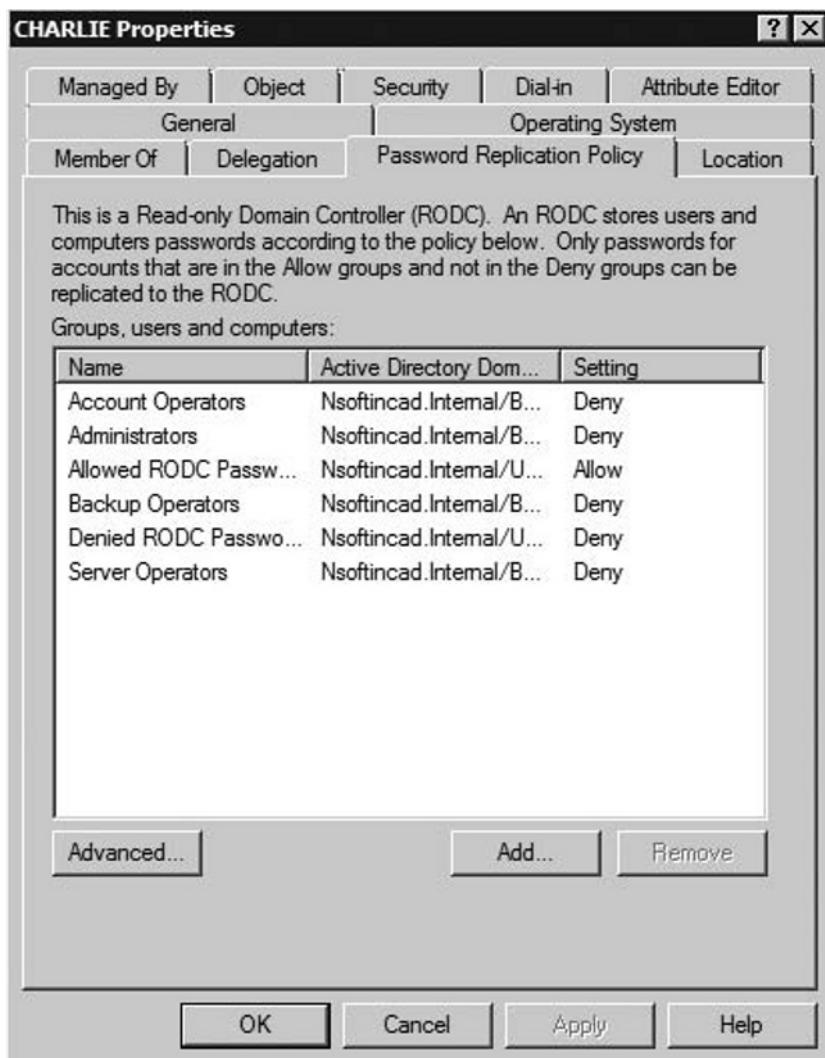
- Allowed RODC Password Replication Group
- Denied RODC Password Replication Group

These two groups are added automatically to every Password Replication Policy and therefore allow you to specify a default Allow and Deny List for all your RODCs (see Figure 6.22). Of course it is possible to remove these groups from a Password Replication Policy if necessary.

The *Allowed RODC Password Replication Group* has no members by default. The *Denied RODC Password Replication Group* contains the following members by default:

- Cert Publishers
- Domain Admins
- Domain Controllers
- Enterprise Admins
- Group Policy Creator Owners
- krbtgt (Domain-Wide Kerberos Ticket Account)
- Read-only Domain Controllers
- Schema Admins

Figure 6.22 Password Replication Policy Opened in Active Directory Users and Computers



EXAM WARNING

Remember that both the *Allowed RODC Password Replication Group* and the *Denied RODC Password Replication Group* are domain local groups. Domain local groups cannot contain built-in groups. This is why groups such as *Account Operators* have explicit entries in the password replication policy.



TEST DAY TIP

Password Replication Policies are stored in Active Directory. Therefore, you can change them only on a writable copy of Active Directory. Please keep in mind that after you change a password replication policy, depending on your replication topology, it might take a while until your changes become effective on the RODC! To speed up the process you can trigger Active Directory replication.

EXERCISE 6.14

ADDING AN ALLOW ENTRY TO A PASSWORD REPLICATION POLICY

1. Logon as a domain administrator on a writeable domain controller.
2. Click Start | Administrative Tools | Active Directory Users and Computers.
3. In Active Directory Users and Computers select the **Domain Controllers OU**.
4. In the Domain Controllers OU right-click an RODC computer object and select **Properties**.
5. In the <computername> properties dialog select the **Password Replication Policy Tab**.
6. On the password replication policy tab click **Add**.
7. Select **Allow password for the account to replicate to this RODC** (see Figure 6.23) and click **OK**.

Figure 6.23 Choosing the Password Replication Setting

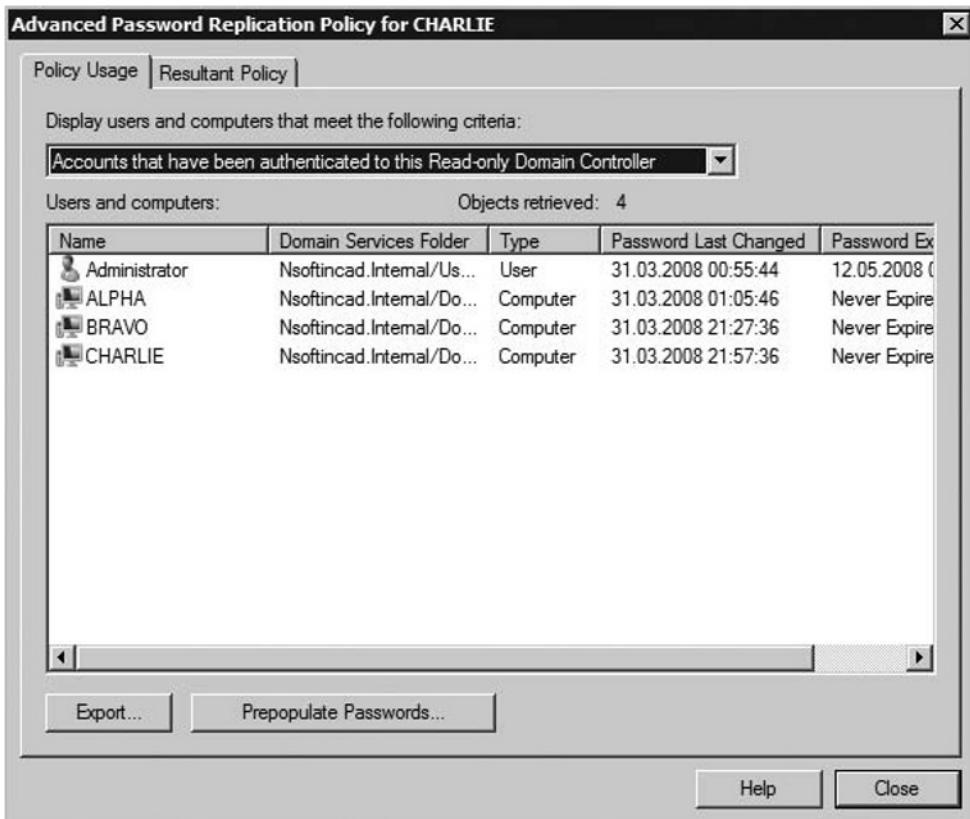


8. In the Select Users, Computers, or Groups box enter a **username** and click **OK**.
 9. Click **OK**.
-

Examining Cached Credentials

In complex environments, with several entries in a password replication policy, keeping track of all the cached credentials can become difficult. Just think of group nesting, multiple group membership, and so on. To help administrators with this problem, Microsoft added functionality to examine cached credentials on an RODC. Using this functionality it is possible to view accounts that are cached on an RODC or view accounts that have been authenticated to an RODC (see Figure 6.24). In large organizations, the list of cached or authenticated accounts may be quite large. An export function comes to the rescue for these environments.

Figure 6.24 Examining Authenticated Accounts on an RODC



To Export a List of Cached Accounts

1. Log on to any working DC.
2. Click **Start | Administrative Tools | Active Directory Users and Computers**.
3. In Active Directory Users and Computers select the **Domain Controllers OU**.
4. Right-click an RODC **computer account** and select **Properties**.
5. Select the **Password Replication Policy** tab and click **Advanced**.
6. In the drop-down box make sure that **Accounts whose passwords are stored on this Read-only Domain Controller** is selected.
7. In the **Filename** box input **filename** and click **Save**.

TEST DAY TIP

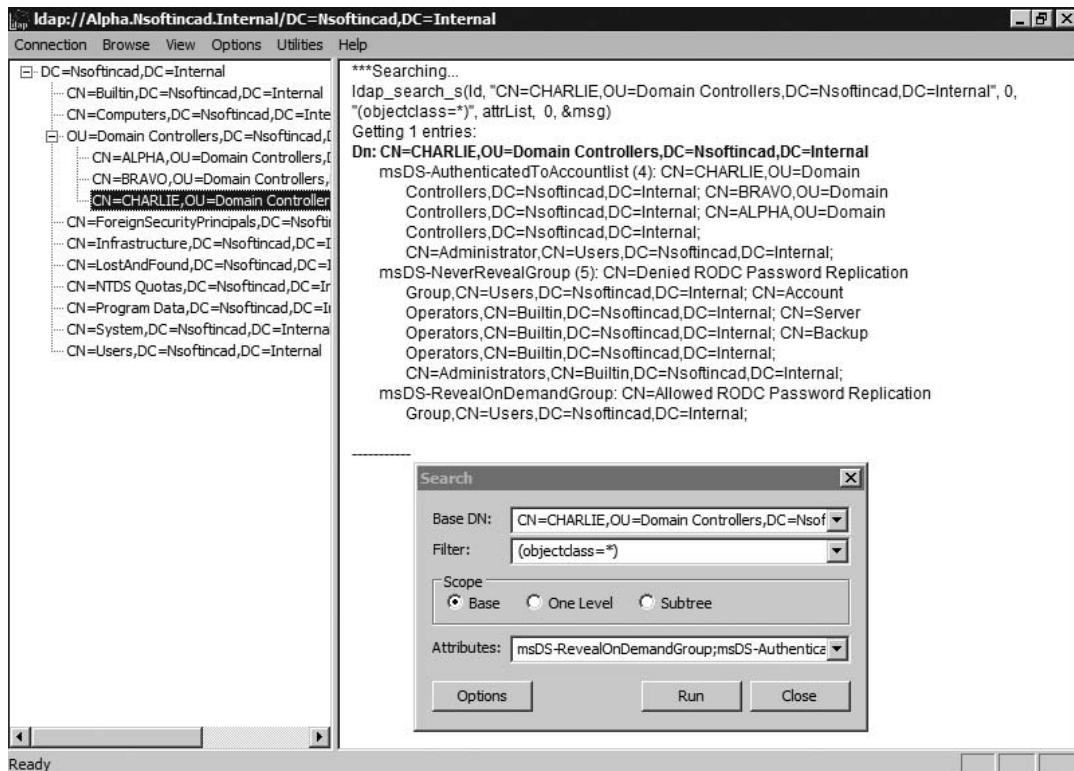
You can also prepopulate passwords on an RODC. This is done on a per-user basis. Prepopulation is permitted only for accounts that have an allow entry in the password replication policy. To prepopulate a password, open the password replication policy as mentioned in the preceding exercise, click **Advanced**, and then click **Prepopulate Passwords**.

Where Is a Password Replication Policy Stored?

A Password Replication Policy is stored in Active Directory in the following four multivalued AD DS attributes on each RODC:

- msDS-Reveal-OnDemandGroup, stores all allowed accounts
- msDS-NeverRevealGroup, stores all denied accounts
- msDS-RevealedUsers, stores a list of accounts that are always stored locally
- msDS-AuthenticatedToAccountList, stores a list of accounts that have been authenticated to the RODC

These attributes store security principals (user, groups or computers) as distinguished names or SIDs (see Figure 6.25).

Figure 6.25 Password Replication Policy Attributes Revealed with LDP.EXE

Designing Password Replication Policies

Designing a Password Replication strategy means you have to decide which and how many user account credentials should be replicated to an RODC. Several factors influence your RODC authentication strategy:

- Security
- User count at the remote location
- Manageability
- Network reliability

There are three scenarios or models, which you can implement (all of which deny credential caching for administrative accounts!), as shown in Table 6.4.

Table 6.4 Password Replication Policy Strategies

| Model | Pros | Cons |
|-------------------------|---|---|
| No Account caching | Secure. Policy Processing is local to the site. Authentication is fast. | Relies on availability of the WAN connection. No user authentication when WAN connection fails. |
| Full Account caching | No reliance on WAN availability. Very low impact on WAN bandwidth. Mostly for manageability (Role Separation) | Possible security breach. |
| Branch-specific caching | Allows fine-grain control over stored credentials. Authentication for branch users even if WAN link fails. | Need to monitor authentication requests to RODC. Tweak of replication policy necessary to accommodate additional authentication requests. |

Let's explain these models in more detail.

No Account Caching

This is the most secure model. It only replicates the RODC computer account and special Kerberos accounts credentials. However, account authentication relies on WAN availability. From an administrative point of view, this model needs the least administration. No additional configuration is required after the RODC is promoted. For security purposes, administrators could deny credential caching for their own security-sensitive user groups.

Full Account Caching

In this model, most of the user accounts in Active Directory have their password stored on an RODC. This can be achieved by adding the Domain Users group or a group that contains a majority of the user accounts to the allow list. The default deny settings in the password replication policy still apply. Hence, passwords of

members of the Domain Admins group and similar groups are not cached on the RODC. This model allows for offline operation (e.g., authentication even if the WAN link fails). It is most appropriate for environments where the physical security of an RODC is not at risk.

Branch-Specific Caching

In this scenario, only passwords of users who work in the branch office are stored on the RODC. It is achieved by adding a branch specific group to the allowed list and by adding the branch users to this group. Of course the administrator could also add single users to the allow list, although this is not recommended. Combined with Role Separation this model eases administration in the branch by leveraging delegated User and Group Account Management: by changing the membership of the branch specific group, the delegated administrator automatically is permitted to modify the list of accounts for which passwords are cached on the RODC.

Under certain circumstances, it might be necessary that administrators examine the “Authenticated to” list on the password replication policy in Active Directory, to identify accounts that should be added to the allowed list.

Role Separation

In Windows 2000 Server and Windows Server 2003 Active Directory, delegation of administrative permissions on a domain controller computer was nearly impossible.

For example, you can easily delegate administrative authority for a complete organization unit structure to a trustworthy user in a remote site. But this only allows for Active Directory administration—managing users, groups, and such. It doesn’t allow for *local* administration on the domain controller itself. The trusted account would not be able to log on to the domain controller, patch the system, and so on.

We could argue that this should be no problem because you could add the trusted entity to the *Administrators* group that is permitted to administer the domain controller locally. Theoretically, this is true. However, the downside is that by adding the user to the *Administrators* group in Active Directory, you not only allow the user to administer the local domain controller, you allow administration of *all* domain controllers in the domain *and* (!) allow the user to administer your complete Active Directory infrastructure. The same rule applies to all built-in groups in Active Directory (*server operators*, etc.). Do you really want to do this? I think we failed the goal here!

The reason behind this is that there are no *local* groups on normal domain controllers to control who can administer a domain controller. Instead, the membership

of the built-in groups is replicated to any DC in the same domain. This is not a failure or a bug—it is implicit to Active Directory replication.

To address this problem, Microsoft introduced the so-called “role separation” in Windows Server 2008 Active Directory. Role separation gives the administrator the ability to delegate local administrator permissions on an RODC. So in our previous example, the trusted user could be added to the *local* administrators group on the RODC, log on locally to the RODC, and perform maintenance tasks, and others.

The implementation of this feature might be somewhat confusing. I am sure in the past you have learned that domain controllers do not have local users or groups (as member servers and workstations do). Why does an RODC have local administrators? Local groups on an RODC are also referred to as *Roles*—therefore the name role separation. The important thing here is not to confuse local groups on an RODC with the local accounts database on a member server or workstation (also known as *Security Accounts Manager*, or *SAM*). They are completely different! More important, role separation is available only on RODCs. You could configure role separation on a *normal* domain controller, but it would have no effect at all.

If you add a user to the local role *administrators* on an RODC, the change is written to the registry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\control\lsa\rodroles  
Name: 544  
Data type: REG_MULTI_SZ  
Value: S-1-5-21-760266474-1386482297-4237089879-1107
```

The Relative Identifier (RID) of the corresponding group in Windows denotes the role name. In our example 544 is the well-known RID of the built-in\administrators group. Then, each value represents the security identifier (SID) of a user who has been assigned to the role.

Role separation is configured with **NTDSUTIL**. It can either be managed locally on the RODC itself or remotely by connection to the RODC within **NTDSUTIL**.

NOTE

Any user account added to the local administrators role is permitted to administer all aspects of the local system. These administrators also have the ability to add or remove accounts from any local role. They are not permitted to deny the Domain Admins group any rights in an RODC.

Configuring Role Separation

To add an account to the local administrator's role:

1. Log on to any working RODC.
2. Click **Start | Run**, type **ntdsutil** in the Open box, and then click **OK**.
3. Type **local roles** and press **Enter**.
4. Type **add NSOFTINCAD\Tariq administrators** and press **Enter**.

To further check the membership of the local administrator's role:

1. Type **show role administrators**, and press **Enter**.
2. Type **Quit** and press **Enter**.
3. Type **Quit** and press **Enter**. See Figure 6.26.

Figure 6.26 Examining Local Roles

```
C:\Users\Administrator.NSOFTINCAD>ntdsutil
ntdsutil: local roles
local roles: show role administrators
  NSOFTINCAD\tariq
local roles:
```

Remote Administration

Before you deploy your servers you need to determine to which extent you need to manage them remotely. Windows Server 2008 supports a wide range of built-in remote management tools that you can use to manage servers. These tools are used when the server is functioning and you have access over the standard network connection. Some of the tools you might consider for remote management are:

- Remote desktop for administration
- Remote server administration tools
- Telnet
- Windows remote management (WinRM)
- Group policy

In case your server is not reachable by means of the standard network connection, you probably have to use Emergency Management Service (built into Windows Server 2003 and 2008), together with other hardware and software solutions, to bring the system back into production.

When Emergency Management Service (EMS) is enabled, all administrative tasks should be possible via a remote console that is connected over a serial port. EMS can be enabled by modifying the boot configuration data store with the **bcdedit** tool.

Remote Desktop for Administration

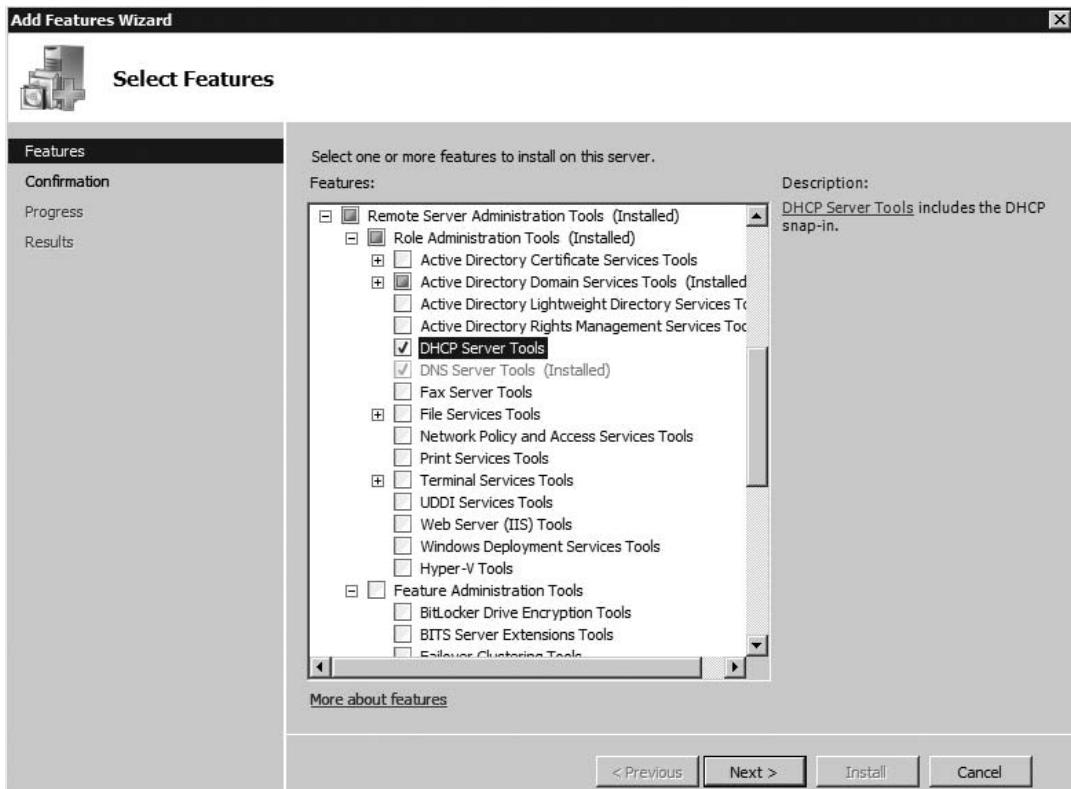
Remote Desktop for administration provides a convenient way of remotely administering a server. It has low bandwidth requirements, presents the administrator with a familiar environment and allows the mapping of local drives, printer, and the like into the remote session.

Changes to the security system in Windows Vista as well as Windows Server 2008 result in some differences in the administration experience. If you want to connect to the console in Windows Server 2008 via Remote Desktop Client, you have to use the command switch **/admin**. Although the **/console** switch still exists, it doesn't have any effect. Another change is the fact that any user is restricted to one remote desktop session. However, this behavior can be changed in the terminal services configuration.

Remote Server Administration Tools

Formerly known as Administration Tools Pack, Remote Server Administration Tools (RSAT) are the replacement for the server administration tools that can be installed on a Windows system. But not only the name has changed—also the install package is different. **ADMINPAK.MSI** (the administration tools pack) does no longer exist for Windows Vista and Windows Server 2008. Instead, RSAT is an integral part of Windows Server 2008 and is an optional download for Windows Vista Service Pack 1. RSAT on Windows Server 2008 are a *feature* and can be installed with Server Manager (see Figure 6.27).

Figure 6.27 Remote Server Administration Tools Installation in Server Manager



Telnet

Telnet is a well-known, global, and versatile tool that has been used by systems administrators for decades. In the past used mostly by UNIX administrators, it has also become very popular to Windows administrators since it provides interoperability with operating systems other than windows.

Telnet traffic is by itself not encrypted and therefore provides little security when used over shared networks. Thus neither the Telnet client component nor the Server component are installed on Windows Server 2008 by default, but can be installed easily via Server Manager.

A more secure alternative is Secure Shell (SSH), which allows data exchange over a secure channel. SSH uses public-key cryptography to authenticate the user. It also supports mutual authentication in that the remote system authenticates the user.

However, SSH has inherent design flaws and more and more is replaced by SSH2. SSH2 is an Internet Engineering Task Force Standard.

Windows Remote Management (WinRM)

Historically Windows operating systems always have lacked support for remote management from the command shell. Several utilities exist to manage a system locally—a few of them also provide remote management capabilities—to some degree. A very popular way of managing or automating a system remotely is the use of WMI. Don’t get me wrong—there’s nothing wrong with WMI itself. It is just the way you interact with the system. You either use the WMI command shell or write your own scripts.

And have you ever thought about the network-side of WMI? WMI relies on DCOM. So what is the downside to DCOM? Well, DCOM works great on your local network. But as soon as you communicate outside your network this can become a real problem. Most firewalls block the DCOM protocol. Of course it’s possible to open the specific ports for DCOM; the downside to this is that the bad guys (e.g., hackers) also use DCOM! Of course you can help yourself by using a free implementation of Secure Shell (SSH). But wouldn’t it be nice if Windows had some stuff built-in? The wait is over: Windows Remote Management (WinRM) comes to the rescue!

WinRM is Microsoft’s implementation of the WS-Management protocol, which is a Simple Object Access Protocol (SOAP), which is an extension to the HTTP protocol. Isn’t that beautiful? It uses HTTP or HTTPS—standard protocols that typically firewalls do not block. Another advantage is that you can route the protocol through a proxy server. Since WS-Management is a standard, it theoretically allows you to open a remote shell on *any* system that is capable of communicating via the WS-Management protocol. In addition to that, on Windows Systems it allows the execution of WMI scripts without opening DCOM ports. WinRM had its debut in Windows Server 2003 R2, it is built into Vista and Windows Server 2008, and is available as an optional download for Windows XP Service Pack 2 and Windows Server 2003 Service Pack 1.

WinRM Listeners

To enable WinRM you have to create a *listener*, which acts as a HTTP-interface. Be aware that the default listener uses HTTP and therefore is not secured! If you want to secure a WinRM listener, you have to enroll a certificate for server authentication and then configure the listener to use this certificate.

WinRM listeners provide several authentication mechanisms: Basic Authentication, Digest, and Negotiating. Negotiating is the default and will use Kerberos or NTLM. For Basic or Digest authentication to work you are forced to install a certificate.

EXERCISE 6.15

ENABLING WINRM

1. Log on as an administrator.
2. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. At the command prompt, type **winrm quickconfig**.
4. Type **Y** to enable WinRM.

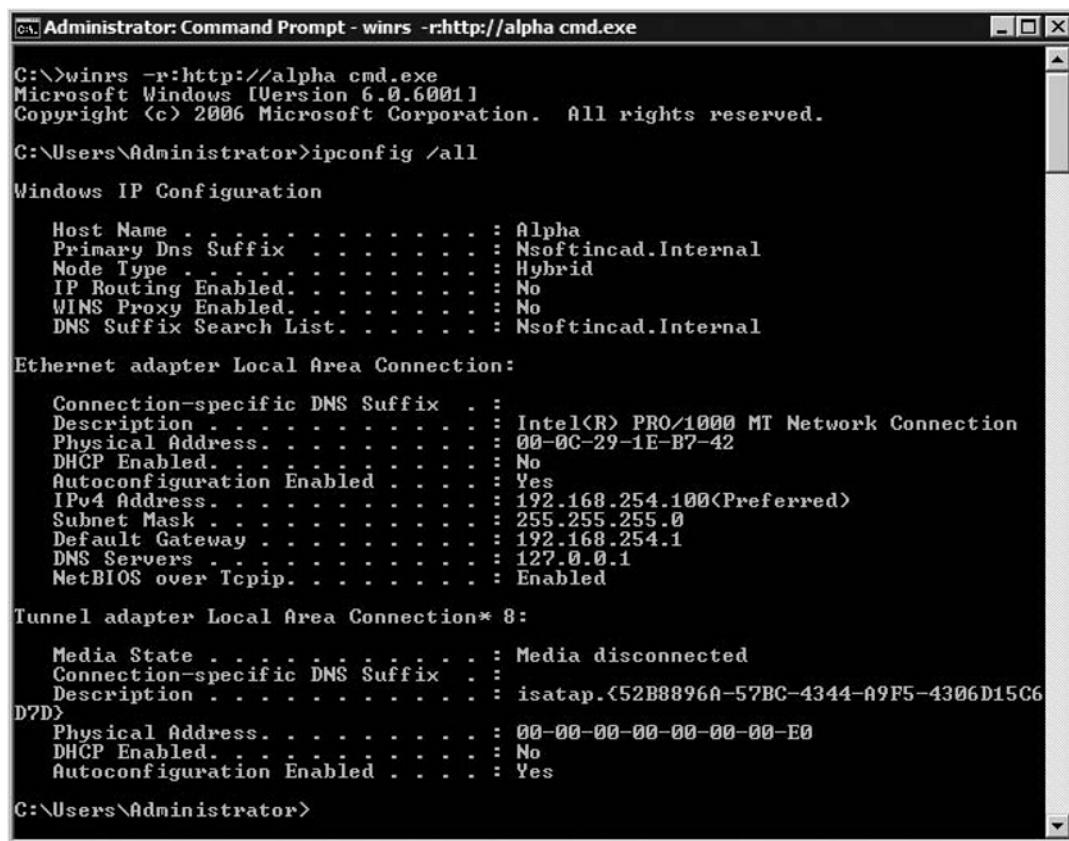
Remote Management Using WinRM

Remote management with WinRM uses a client component **winrs** to connect to the WinRM enabled system.

EXERCISE 6.16

REMOTE MANAGEMENT WITH WINRS

1. Logon as an administrator.
2. Click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**.
3. On the command prompt type **winrs -r:http://<hostname> cmd.exe**. A new command prompt should open on the remote system.
4. Type **ipconfig /all**. The output (e.g., IP address information) should be from the remote system (see Figure 6.28).

Figure 6.28 WinRS: Ipconfig Output from a Remote Host


The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - winrs -r:http://alpha cmd.exe". The output of the ipconfig /all command is displayed, showing network configuration details for two adapters: "Local Area Connection" and "Local Area Connection* 8".

```
C:\>winrs -r:http://alpha cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\>Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : Alpha
Primary Dns Suffix . . . . . : Nsoftincad.Internal
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : Nsoftincad.Internal

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-1E-B7-42
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 192.168.254.100<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.254.1
DNS Servers . . . . . : 127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 8:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : isatap.{52B8896A-57BC-4344-A9F5-4306D15C6D7D}
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\>Users\Administrator>
```

5. Type **exit** to disconnect from the remote system.

Group Policy

Group Policy offers a wide range of configuration options, such as software installation, security settings, file system and registry permissions, scripts for startup and shutdown, and management of registry settings. In Windows Server 2008, Microsoft extended group policy with Group Policy Preferences. GPO Preferences allows you to extend GPO settings such as the advanced management of the registry, mapping of network drives, management of environment variables, and regional options. The biggest advantage of GPO Preferences is that it saves you from creating your own Group Policy Settings templates, also known as ADM or ADMX files.

Summary of Exam Objectives

Branch offices have special requirements in terms of design and deployment. The topology used for most branch office deployments is a hub and spoke topology. When you design an authentication strategy for a branch, consider the following:

- Physical security
- User population
- Availability of technical expertise on-site
- WAN link speed and bandwidth utilization
- Active Directory aware applications

Although Active Directory replication between sites is compressed and can be scheduled, replication traffic can negatively affect logon performance if clients log on over a WAN link. If logon times exceed an acceptable limit, consider placing a domain controller in the remote office. Global Catalog Servers cause additional replication traffic over the WAN link. If the installation of a Global Catalog server in a branch office is not feasible, universal group membership is good alternative. Universal Group membership caching retrieves a user's universal group membership at first logon and stores it as an attribute of the user object in Active Directory.

Finally, full domain controllers should be installed in branch offices only if applications write directly to the directory or use synchronous protocols such as DCOM and RPC to communicate with the domain controller.

Windows BitLocker provides enhanced protection for operating system and user data in branch offices. It encrypts both operating system and data volumes and checks the integrity of early boot components and boot configuration data. It provides remote administration interfaces and rich recovery mechanisms.

BitLocker requires a Trusted Platform (TPM) for its full functionality. A TPM is an integrated circuit that includes a nearly nondestructable RSA key. It is designed to generate cryptographic keys and random numbers to perform functions like Secure I/O, memory curtaining, remote attestation, and sealed storage. Secure I/O makes sure that a user cannot copy data while it is processed by an application. Memory curtaining provides enhanced memory protection. Remote attestation detects changes in computer hardware and software. Information protected by sealed storage can only be read on authorized systems.

BitLocker full volume encryption is transparent to the user and minimally affects the performance of a system. In Windows Server 2008, BitLocker supports

drive encryption in contrast to Windows Vista, which only supports volume encryption. Full volume encryption uses three keys for its operation: the full volume encryption key, the volume master key, and the key stored on the TPM.

The BitLocker integrity check makes sure that none of the startup components has changed. Startup components encompass the BIOS, the master boot record, the boot sector, and the boot manager code. If you move a BitLocker protected disk to another system, the disk cannot be read, because startup data has changed.

To improve security, BitLocker supports multifactor authentication methods for computer startup. In addition to a TPM, multifactor authentication requires a PIN or a startup key at computer startup. Startup keys are stored on USB media such as flash drives.

To enable BitLocker on your system you need two partitions, a 1.5 GB partition that is set active. It becomes the startup partition and is not encrypted and a second partition for installing the operating system. To install BitLocker you select the BitLocker Drive Encryption feature in Server Manager. After the installation, you must reboot the system.

When you turn on BitLocker in control panel, the system creates a recovery password. The password must be stored on a USB drive or a network drive and can also be printed. You can encrypt data volumes only if the operating system volume is encrypted. Encryption of data volumes is enabled with the script **manage-bde.wsf**.

You can configure BitLocker for operation without a TPM. However, without a TPM, BitLocker cannot check the integrity of startup components and only provides volume encryption. Operation without a TPM is configured with Group Policies. TPM-less operation requires a startup key stored on a USB drive.

TPM owner passwords, encryption keys, and recovery passwords can be backed up in Active Directory. To use Active Directory for BitLocker backup you have to extend the Active Directory schema. Furthermore, you need to set permissions in the domain to allow the storage of TPM passwords and configure group policy settings to BitLocker Active Directory backup on the client.

Usage of read-only domain controllers (RODC) can enhance the security of Active Directory in branch offices. Changes cannot be written to the read-only Active Directory database on an RODC. Instead, you have to connect to a writable domain controller to make changes. Changes are replicated during normal replication cycles. Passwords are not stored on an RODC by default. During user authentication, an RODC connects to a writable domain controller in a direct connected site. The writeable DC validates these credentials and passes them back to the RODC.

Although by default no passwords are stored on an RODC, password storage is configurable via password replication policies. A password replication policy is a list of accounts for which the password is permitted or denied from being replicated to an RODC. Each RODC has its unique password replication policy. Password replication policies contain several deny entries by default. These deny entries make sure that no administrative passwords are stored on a domain controller. The groups “Allowed RODC Password Replication” and “Denied RODC Password Replication” automatically appear in each password replication. They allow you to define a default allow and deny list for all RODCs. When you permit a password for replication, it replicates at first logon. We call this process credential caching.

RODCs also support the DNS role. RODC hosts a read-only Active Directory integrated DNS zone that does not accept updates. Clients updating their DNS records obtain a redirection to a writable copy of DNS.

Installation of an RODC involves the same steps as installing a full domain controller. By prestaging an RODC computer account, you have the ability to delegate the installation of an RODC to a domain user. RODC installation on server core requires an unattended file.

Role separation gives the administrator the flexibility to assign administrative rights for an RODC to a domain user without granting any administrative rights for the domain or other domain controllers. You configure role separation with NTDSUTIL.

Remote management is very important if you operate a dispersed network. Windows Server 2008 includes many powerful remote administration tools:

- Remote Desktop
- Remote Server Administration Tools (RSAT)
- Telnet
- Windows Remote Management (WinRM)
- Group Policy

Remote Server Administration Tools are the replacement for the formerly known ADMINPAK. RSAT is included in Windows Server 2008 and is optional for Windows Vista Service Pack 1.

Windows Remote Management is based on the WS-Management standard and provides remote administration capabilities over HTTP or HTTPS transports. WinRS is the client component used to initiate a connection to a WinRM-enabled host. WinRM is included in Windows Server 2008 and Windows Server 2003 R2 and is downloadable for other windows platforms.

Exam Objectives Fast Track

Developing an Authentication Strategy

- An authentication strategy is a plan that defines the placement of domain controllers.
- Domain controller placement depends on multiple factors such as network bandwidth, user population, number of GPOs, and Active Directory replication.
- Global Catalog Servers should be placed only in remote locations where enough bandwidth is available.
- Read-only domain controllers can enhance the security of branch offices.

Using BitLocker

- In Windows Server 2008, BitLocker supports drive encryption.
- To use BitLocker you need to configure two partitions before you install the operating system.
- BitLocker cannot protect a computer against viruses or malware?
- You can configure Active Directory to back up BitLocker and TPM information.

Configuring Read-Only Domain Controllers

- Read-only domain controllers host a read-only copy of Active Directory and therefore provide enhanced security.
- Authentication on an RODC controller requires a writable domain controller.
- Credential caching allows for storage of account passwords on Read-only domain controllers.
- To define which passwords will be cached on an RODC you use password replication policies.
- In a delegation scenario, you use role separation to assign a normal user account administration rights on an RODC.

Exam Objectives

Frequently Asked Questions

Q: Is there an algorithm I can use to determine if I need to place a domain controller in a remote location?

A: There are some algorithms available on the Internet, although finding a generic algorithm that fits all scenarios might be hard. In real world scenarios, the decision to place a domain controller in a remote office often is influenced by personal experience.

Q: Can I activate Universal Group membership caching on an RODC?

A: Yes, this feature also is supported on an RODC.

Q: Can other tools that manage or modify the master boot record work with BitLocker?

A: Use of other startup managers is not supported by Microsoft.

Q: Approximately, how long will initial encryption take when BitLocker is enabled?

A: BitLocker encryption proceeds at the rate of about 1 gigabyte (GB) per minute in most cases.

Q: I want to change the bit length of the keys that BitLocker uses. Where can I configure this?

A: You can change BitLocker key lengths through group policy. In the group policy management editor console navigate to **Computer Configuration/Policies/Administrative Templates/Windows Components/BitLocker Drive Encryption**. The Policy **Configure encryption method** allows you to change the key length used for BitLocker.

Q: What happens to unallocated space when I enable BitLocker on my volume? Does it get encrypted?

A: BitLocker creates a file that takes most of the available disk space (leaving 6 GB for short-term system needs) and wiping disk sectors that belong to the file. Everything else (including ~6 GB of free space not occupied by the wipe file) is encrypted. When encryption of the volume is paused or completed, the wipe file is deleted and the amount of available free space reverts to normal.

Q: Is it possible to have an RODC host any FSMO Roles?

A: No, this is not possible. For example the RID Master assigns RID-Pools to each DC and updates the pool information in AD. On an RODC, this update would fail since the database is read-only.

Q: Does Microsoft Exchange Server use an RODC that is configured as a Global Catalog?

A: Neither Exchange 2007 nor Exchange 2003 will use an RODC GC for directory operations.

Q: Does SYSVOL replication work on an RODC?

A: SYSVOL replication on an RODC is no different than on normal DCs. It uses FRS and DFS-R to replicate.

Q: Is there any difference in Group Policy processing when a client logs on using an RODC?

A: Since an RODC also hosts a complete replica of the SYSVOL share, processing of Group Policies is not different.

Self Test

1. You have been asked to design a branch office deployment for your company. Which of the following might influence your design?
 - A. User population
 - B. WAN link availability
 - C. Physical security
 - D. Technical on-site expertise
2. Your company is implementing Read-only Domain Controllers. You install a Windows Server 2008 domain controller in your domain to support installation of RODCs. Which FSMO role should you assign to this domain controller?
 - A. RID master
 - B. Infrastructure master
 - C. Schema master
 - D. PDC emulator
 - E. Domain naming master
3. Alice works as a system administrator at a company called Wiredworld. She wants to prepare Active Directory for RODC operation. Which steps does she need to take to prepare Active Directory for RODC operation?
 - A. Raise the Forest functionality level to Windows Server 2003
 - B. Raise the Domain functionality level to Windows Server 2008
 - C. Prepare Active Directory by running adprep/rodcprep
 - D. Transfer the PDC Emulator FSMO role to a Windows Server 2008 domain controller
4. As a branch office administrator, you have been asked to complete the installation of a prestaged Read-only domain controller on a server core machine. Which command would you use to start the installation?
 - A. dcpromo /AttachAccount
 - B. dcpromo /InstallPrestagedAccount
 - C. dcpromo /UseExistingAccount:Attach
 - D. dcpromo /CompletePrestaging

5. Bart is a systems administrator at xxx. The network consists of several sites in which RODCs are deployed. Bart wants to prepopulate passwords for users that must be authenticated on all RODCs at all times. He creates a new group and adds the required users as members. After that, he adds a new allow entry for the group to every RODC. A few minutes later, he tries to prepopulate users' passwords and receives an error. What else must he do to be able to prepopulate the users' passwords?
 - A. Add an individual allow entry for every user
 - B. Initiate Active Directory replication
 - C. Add the allow entry directly on the RODC
 - D. Wait for replication to finish
6. James is a Systems administrator for an Active Directory environment. The domain functional level is Windows Server 2008. John wants to enable Active Directory backup for BitLocker and TPM modules. Which steps does he need to take? (choose all that apply)
 - A. Extend the Active Directory schema
 - B. Add permissions on the domain container
 - C. Add users to the "Allow BitLocker Backup" Group in Active Directory
 - D. Configure Group Policy settings for BitLocker and TPM Active Directory backup
7. You are the systems administrator of an Active Directory domain. All Servers are running Windows Server 2008 and have TPM compatible hardware. Your company security policy has been updated recently and requires BitLocker drive encryption all server machines. When you want to enable BitLocker on the first server you receive a warning that the drive configuration is unsuitable for BitLocker drive encryption. What options do you have?
 - A. Shrink the operating system partition, create a new partition, activate the new partition, and copy the boot configuration store to the new partition.
 - B. Install the operating system from scratch. Before you start the installation, create the correct partitioning scheme.
 - C. Use the BitLocker Drive Preparation Tool.
 - D. Configure BitLocker to use a USB drive for encryption.

8. What components are validated by BitLocker boot integrity check?
 - A. Master Boot Record
 - B. BIOS
 - C. Boot Configuration Data Store
 - D. Boot Manager Code
 - E. Boot Sector
9. You replace the motherboard of a BitLocker protected computer. When you turn on the computer, the system is locked and does not boot. Which precautions do you have to take in order to replace the motherboard on a BitLocker protected system while keeping data secured?
 - A. Decrypt all protected volumes in Control Panel
 - B. Disable BitLocker in Control Panel
 - C. Remove the TPM module from the old motherboard and plug it into the new motherboard.
 - D. Save the current startup integrity checksum on a USB drive and restore it on the new system.
10. You are the administrator of a large enterprise network. The network contains domain-joined as well as nondomain-joined servers. You use WinRM for remote management. For nondomain servers you configured Basic authentication as the logon method. When you try to connect to a nondomain server, the connection is refused. What else do you have to configure to successfully connect?
 - A. Configure the nondomain server to use negotiation authentication.
 - B. On the nondomain server, request a certificate and configure WinRM to use the certificate for HTTPS.
 - C. On the client, request a certificate and configure WinRS to use the certificate for HTTPS.
 - D. Add an exception for the WinRM listener on the Windows firewall of the nondomain server.

Self Test Quick Answer Key

- | | |
|---------------|---------------|
| 1. A, B, C, D | 6. A, B, D |
| 2. D | 7. B |
| 3. A, C, D | 8. A, B, D, E |
| 4. C | 9. B |
| 5. B, D | 10. B |

This page intentionally left blank

Chapter 7

MCITP Exam 647

Configuring Certificate Services and PKI

Exam objectives in this chapter:

- What Is PKI?
- Analyzing Certificate Needs within the Organization
- Working with Certificate Services
- Working with Templates

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

Computer networks have evolved in recent years to allow an unprecedented sharing of information between individuals, corporations, and even national governments. The need to protect this information has also evolved, and network security has consequently become an essential concern of most system administrators. Even in smaller organizations, the basic goal of preventing unauthorized access while still allowing legitimate information to flow smoothly requires the use of more and more advanced technology.

That being stated, all organizations today rely on networks to access information. These sources of information can range from internal networks to the Internet. Access to information is needed, and this access must be configured to provide information to other organizations that may request it. When we need to make a purchase, for example, we can quickly check out vendors' prices through their Web pages. In order not to allow the competition to get ahead of our organization, we must establish our own Web page for the advertising and ordering of our products. Within any organization, many sites may exist across the country or around the globe. If corporate data is available immediately to employees, much time is saved. In the corporate world, any time saved is also money saved.

In the mid 1990s, Microsoft began developing what was to become a comprehensive security system of authentication protocols and technology based on already developed cryptography standards known as public key infrastructure (PKI). In Windows 2000, Microsoft used various standards to create the first Windows-proprietary PKI—one that could be implemented completely without using third-party companies. Windows Server 2008 expands and improves on that original design in several significant ways, which we'll discuss later in this chapter.

PKI is the method of choice for handling authentication issues in large enterprise-level organizations today. Windows Server 2008 includes the tools you need to create a PKI for your company and issue digital certificates to users, computers, and applications. This chapter addresses the complex issues involved in planning a certificate-based PKI. We'll provide an overview of the basic terminology and concepts relating to the public key infrastructure, and you'll learn about public key cryptography and how it is used to authenticate the identity of users, computers, and applications/services. We'll discuss different components of PKI, including private key, public key, and a trusted third party (TTP) along with PKI enhancements in Windows Server 2008. We'll discuss the role of digital certificates and the different types of certificates (user, machine, and application certificates).

You'll learn about certification authorities (CAs), the servers that issue certificates, including both public CAs and private CAs, such as the ones you can implement on your own network using Server 2008's certificate services. Next, we'll discuss the CA hierarchy and how root CAs and subordinate CAs act together to provide for your organization's certificate needs. You'll find out how the Microsoft certificate services work, and we'll walk you through the steps involved in implementing one or more certification authorities based on the needs of the organization. You'll learn to determine the appropriate CA type—enterprise or stand-alone CA—for a given situation and how to plan the CA hierarchy and provide for security of your CAs. We'll show you how to plan for enrollment and distribution of certificates, including the use of certificate requests, role-based administration, and autoenrollment deployment.

Next, we'll discuss how to implement certificate templates, different types of templates that you can use in your environment. Finally, we'll discuss the role of key recovery agent and how it works in a Windows Server 2008 environment.

What Is PKI?

The rapid growth of Internet use has given rise to new security concerns. Any company that does not configure a strong security infrastructure is literally putting the company at risk. An unscrupulous person could, if security were lax, steal information or modify business information in a way that could result in major financial disaster. To protect the organization's information, the middleman must be eliminated. Cryptographic technologies such as public key infrastructure (PKI) provide a way to identify both users and servers during network use.

PKI is the underlying cryptography system that enables users or computers that have never been in trusted communication before to validate themselves by referencing an association to a trusted third party (TTP). Once this verification is complete, the users and computers can now securely send messages, receive messages, and engage in transactions that include the interchange of data.

PKI is used in both private networks (intranets) and on the World Wide Web (the Internet). It is actually the latter, the Internet, that has driven the need for better methods for verifying credentials and authenticating users. Consider the vast number of transactions that take place every day over the internet—from banking to shopping to accessing databases and sending messages or files. Each of these transactions involves at least two parties. The problem lies in the verification of who those parties are and the choice of whether to trust them with your credentials and information.

The PKI verification process is based on the use of *keys*, unique bits of data that serve one purpose: identifying the owner of the key. Every user of PKI actually generates or receives two types of keys: a *public key* and a *private key*. The two are actually connected and are referred to as a *key pair*. As the name suggests, the public key is made openly available to the public while the private key is limited to the actual owner of the key pair. Through the use of these keys, messages can be *encrypted* and *decrypted*, allowing data to be exchanged securely (this process will be covered in a few sections later in this chapter).

The use of PKI on the World Wide Web is so pervasive that it is likely that every Internet user has used it without even being aware of it. However, PKI is not simply limited to the Web; applications such as Pretty Good Privacy (PGP) also leverage the basis of PKI technology for e-mail protection; FTP over SSL/TLS uses PKI, and many other protocols have the ability to manage the verification of identities through the use of key-based technology. Companies such as VeriSign and Entrust exist as trusted third-party vendors, enabling a world of online users who are strangers to find a common point of reference for establishing confidentiality, message integrity, and user authentication. Literally millions of secured online transactions take place every day leveraging their services within a public key infrastructure.

Technology aside, PKI fundamentally addresses relational matters within communications. Specifically, PKI seeks to provide solutions for the following:

- Proper authentication
- Trust
- Confidentiality
- Integrity
- Nonrepudiation

By using the core PKI elements of public key cryptography, digital signatures, and certificates, you can ensure that all these equally important goals can be met successfully. The good news is that the majority of the work involved in implementing these elements under Windows Server 2008 is taken care of automatically by the operating system and is done behind the scenes.

The first goal, proper *authentication*, means that you can be highly certain that an entity such as a user or a computer is indeed the entity he, she, or it is claiming to be. Think of a bank. If you wanted to cash a large check, the teller will more than likely ask for some identification. If you present the teller with a driver's license and the picture on it matches your face, the teller can then be highly certain that you are that person—that is, if the teller trusts the validity of the license itself. Because the driver's

license is issued by a government agency—a trusted third party—the teller is more likely to accept it as valid proof of your identity than if you presented an employee ID card issued by a small company that the teller has never heard of. As you can see, trust and authentication work hand in hand.

When transferring data across a network, *confidentiality* ensures that the data cannot be viewed and understood by any third party. The data might be anything from an e-mail message to a database of social security numbers. In the last 20 years, more effort has been spent trying to achieve this goal (data confidentiality) than perhaps all the others combined. In fact, the entire scientific field of cryptology is devoted to ensuring confidentiality (as well as all the other PKI goals).



NOTE

Cryptography refers to the process of encrypting data; *cryptanalysis* is the process of decrypting, or “cracking” cryptographic code. Together, the two make up the science of *cryptology*.

As important as confidentiality is, however, the importance of network data *integrity* should not be underestimated. Consider the extreme implications of a patient’s medical records being intercepted during transmission and then maliciously or accidentally altered before being sent on to their destination. Integrity gives confidence to a recipient that data has arrived in its original form and hasn’t been changed or edited.

Finally we come to *nonrepudiation*. A bit more obscure than the other goals, nonrepudiation allows you to prove that a particular entity sent a particular piece of data. It is impossible for the entity to deny having sent it. It then becomes extremely difficult for an attacker to masquerade as a legitimate user and then send malevolent data across the network. Nonrepudiation is related to, but separate from authentication.

The Function of the PKI

The primary function of the PKI is to address the need for privacy throughout a network. For the administrator, there are many areas that need to be secured. Internal and external authentication, encryption of stored and transmitted files, and e-mail privacy are just a few examples. The infrastructure that Windows Server 2008

provides links many different public key technologies in order to give the IT administrator the power necessary to maintain a secure network.

Most of the functionality of a Windows Server 2008-based PKI comes from a few crucial components, which are described in this chapter. Although there are several third-party vendors such as VeriSign (www.verisign.com) that offer similar technologies and components, using Windows Server 2008 can be a less costly and easier to implement option—especially for small and medium-sized companies.

Components of PKI

In today's network environments, key pairs are used in a variety of different functions. This series will likely cover topics such as virtual private networks (VPNs), digital signatures, access control (SSH), secure e-mail (PGP—mentioned already—and S/MIME), and secure Web access (Secure Sockets Layer, or SSL). Although these technologies are varied in purpose and use, each includes an implementation of PKI for managing trusted communications between a host and a client.

While PKI exists at some level within the innards of several types of communications technologies, its form can change from implementation to implementation. As such, the components necessary for a successful implementation can vary depending on the requirements, but in public key cryptography there is always:

- A private key
- A public key
- A trusted third party (TTP)

Since a public key must be associated with the name of its owner, a data structure known as a public key certificate is used. The certificate typically contains the owner's name, their public key and e-mail address, validity dates for the certificate, the location of revocation information, the location of the issuer's policies, and possibly other affiliate information that identifies the certificate issuer with an organization such as an employer or other institution.

In most cases, the private and public keys are simply referred to as the private and public key certificates, and the trusted third party is commonly known as the certificate authority (CA). The certificate authority is the resource that must be available to both the holder of the private key and the holder of the public key. Entire hierarchies can exist within a public key infrastructure to support the use of multiple certificate authorities.

In addition to certificate authorities and the public and private key certificates they publish, there are a collection of components and functions associated with the

management of the infrastructure. As such, a list of typical components required for a functional public key infrastructure would include but not be limited to the following:

- Digital certificates
- Certification authorities
- Certificate enrollment
- Certificate revocation
- Encryption/cryptography services

Although we have already covered digital certificates and certificate authorities at a high level, it will be well worth our time to revisit these topics. In the sections to follow, we will explore each of the aforementioned topics in greater detail.

New & Noteworthy...

PKI Enhancements in Windows Server 2008

Windows Server 2008 introduces many new enhancements that allow for a more easily implemented PKI solution and, believe it or not, the development of such solutions. Some of these improvements extend to the clients, such as the Windows Vista operating system. Overall, these improvements have increased the manageability throughout Windows PKI. For example, the revocations services have been redesigned, and the attack surface for enrollment has decreased. The following list items include the major highlights:

- **Enterprise PKI (PKIView)** PKIView is a Microsoft Management Console (MMC) snap-in for Windows Server 2008. It can be used to monitor and analyze the health of the certificate authorities and to view details for each certificate authority certificate published in Active Directory Certificate Servers.
- **Web Enrollment** Introduced in Windows Server 2000, the new Web enrollment control is more secure and makes the use of

Continued

scripts much easier. It is also easier to update than previous versions.

- **Network Device Enrollment Service (NDES)** In Windows Server 2008, this service represents Microsoft's implementation of the Simple Certificate Enrollment Protocol (SCEP), a communication protocol that makes it possible for software running on network devices, such as routers and switches that cannot otherwise be authenticated on the network, to enroll for X.509 certificates from a certificate authority.
- **Online Certificate Status Protocol (OCSP)** In cases where conventional CRLs (Certificate Revocation Lists) are not an optimal solution, Online Responders can be configured on a single computer or in an Online Responder Array to manage and distribute revocation status information.
- **Group Policy and PKI** New certificate settings in Group Policy now enable administrators to manage certificate settings from a central location for all the computers in the domain.
- **Cryptography Next Generation** Leveraging the U.S. government's Suite B cryptographic algorithms, which include algorithms for encryption, digital signatures, key exchange, and hashing, Cryptography Next Generation (CNG) offers a flexible development platform that allows IT professionals to create, update, and use custom cryptography algorithms in cryptography-related applications such as Active Directory Certificate Services (AD CS), Secure Sockets Layer (SSL), and Internet Protocol Security (IPsec).

How PKI Works

Before we discuss how PKI works today, it is perhaps helpful to understand the term encryption and how PKI has evolved. The history of general cryptography almost certainly dates back to almost 2000 B.C. when Roman and Greek statesmen used simple alphabet-shifting algorithms to keep government communication private. Through time and civilizations, ciphering text played an important role in wars and politics. As modern times provided new communication methods, scrambling information became increasingly more important. World War II brought about the first use of the computer in the cracking of Germany's Enigma code. In 1952,

President Truman created the National Security Agency at Fort Meade, Maryland. This agency, which is the center of U.S. cryptographic activity, fulfills two important national functions: It protects all military and executive communication from being intercepted, and it intercepts and unscrambles messages sent by other countries.

Although complexity increased, not much changed until the 1970s, when the National Security Agency (NSA) worked with Dr. Horst Feistel to establish the Data Encryption Standard (DES) and Whitfield Diffie and Martin Hellman introduced the first public key cryptography standard. Windows Server 2008 still uses Diffie-Hellman (DH) algorithms for SSL, Transport Layer Security (TLS), and IPsec. Another major force in modern cryptography came about in the late 1970s. RSA Labs, founded by Ronald Rivest, Adi Shamir, and Leonard Adleman, furthered the concept of key cryptography by developing a technology of key pairs, where plaintext that is encrypted by one key can be decrypted only by the other matching key.

There are three types of cryptographic functions. The hash function does not involve the use of a key at all, but it uses a mathematical algorithm on the data in order to scramble it. The secret key method of encryption, which involves the use of a single key, is used to encrypt and decrypt the information and is sometimes referred to as symmetric key cryptography. An excellent example of secret key encryption is the decoder ring you may have had as a child. Any person who obtained your decoder ring could read your “secret” information.

There are basically two types of symmetric algorithms. Block symmetric algorithms work by taking a given length of bits known as blocks. Stream symmetric algorithms operate on a single bit at a time. One well-known block algorithm is DES. Windows 2000 uses a modified DES and performs that operation on 64-bit blocks using every eighth bit for parity. The resulting ciphertext is the same length as the original cleartext. For export purposes the DES is also available with a 40-bit key.

One advantage of secret key encryption is the efficiency with which it takes a large amount of data and encrypts it quite rapidly. Symmetric algorithms can also be easily implemented at the hardware level. The major disadvantage of secret key encryption is that a single key is used for both encryption and decryption. There must be a secure way for the two parties to exchange the one secret key.

In the 1970s this disadvantage of secret key encryption was eliminated through the mathematical implementation of public key encryption. Public key encryption, also referred to as asymmetric cryptography, replaced the one shared key with each user’s own pair of keys. One key is a public key, which is made available to everyone and is used for the encryption process only. The other key in the pair, the private key, is available only to the owner. The private key cannot be created as a result of the public key’s being available. Any data that is encrypted by a public key can be

decrypted only by using the private key of the pair. It is also possible for the owner to use a private key to encrypt sensitive information. If the data is encrypted by using the private key, then the public key in the pair of keys is needed to decrypt the data.

DH algorithms are known collectively as *shared secret key* cryptographies, also known as symmetric key encryption. Let's say we have two users, Greg and Matt, who want to communicate privately. With DH, Greg and Matt each generate a random number. Each of these numbers is known only to the person who generated it. Part one of the DH function changes each secret number into a nonsecret, or public, number. Greg and Matt now exchange the public numbers and then enter them into part two of the DH function. This results in a private key—one that is identical to both users. Using advanced mathematics, this shared secret key can be decrypted only by someone with access to one of the original random numbers. As long as Greg and Matt keep the original numbers hidden, the shared secret key cannot be reversed.

It should be apparent from the many and varied contributing sources to PKI technology that the need for management of this invaluable set of tools would become paramount. If PKI, like any other technology set, continued to develop without standards of any kind, then differing forms and evolutions of the technology would be implemented ad hoc throughout the world. Eventually, the theory holds that some iteration would render communication or operability between different forms impossible. At that point, the cost of standardization would be significant, and the amount of time lost in productivity and reconstruction of PKI systems would be immeasurable.

Thus, a set of standards was developed for PKI. The Public-Key Cryptography Standards (PKCS) are a set of standard protocols used for securing the exchange of information through PKI. The list of these standards was actually established by RSA laboratories—the same organization that developed the original RSA encryption standard—along with a group of participating technology leaders that included Microsoft, Sun, and Apple.

PKCS Standards

Here is a list of active PKCS standards. You will notice that there are gaps in the numbered sequence of these standards, and that is due to the retiring of standards over time since they were first introduced.

- **PKCS #1: RSA Cryptography Standard** Outlines the encryption of data using the RSA algorithm. The purpose of the RSA Cryptography Standard is in the development of digital signatures and digital envelopes. PKCS#1 also describes a syntax for RSA public keys and private keys.

The public-key syntax is used for certificates, while the private-key syntax is used for encrypting private keys.

- **PKCS #3: Diffie-Hellman Key Agreement Standard** Outlines the use of the Diffie-Hellman Key Agreement, a method of sharing a secret key between two parties. The secret key used to encrypt ongoing data transfer between the two parties. Whitefield Diffie and Martin Hellman developed the Diffie-Hellman algorithm in the 1970s as the first public asymmetric cryptographic system (asymmetric cryptography was invented in the United Kingdom earlier in the same decade, but was classified as a military secret). Diffie-Hellman overcomes the issue of symmetric key system, because management of the keys is less difficult.
- **PKCS #5: Password-based Cryptography Standard** A method for encrypting a string with a secret key that is derived from a password. The result of the method is an octet string (a sequence of 8-bit values). PKCS #8 is primarily used for encrypting private keys when they are being transmitted between computers.
- **PKCS #6: Extended-certificate Syntax Standard** Deals with extended certificates. Extended certificates are made up of the X.509 certificate plus additional attributes. The additional attributes and the X.509 certificate can be verified using a single public-key operation. The issuer that signs the extended certificate is the same as the one that signs the X.509 certificate.
- **PKCS #7: Cryptographic Message Syntax Standard** The foundation for Secure/Multipurpose Internet Mail Extensions (S/MIME) standard. It is also compatible with Privacy-Enhanced Mail (PEM) and can be used in several different architectures of key management.
- **PKCS #8: Private-key Information Syntax Standard** Describes a method of communication for private-key information that includes the use of public-key algorithm and additional attributes (similar to PKCS #6). In this case, the attributes can be a DN or a root CA's public key.
- **PKCS #9: Selected Attribute Types** Defines the types of attributes for use in extended certificates (PKCS #6), digitally signed messages (PKCS #7), and private-key information (PKCS #8).

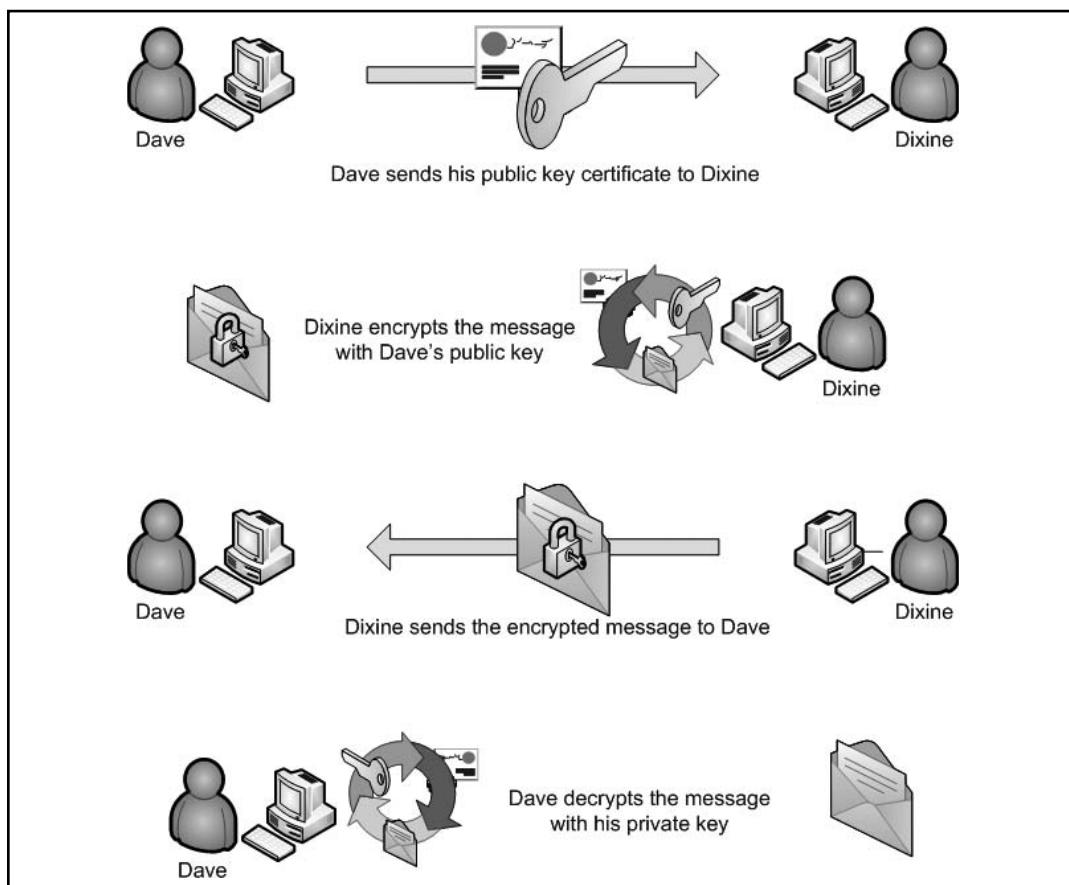
- **PKCS #10: Certification Request Syntax Standard** Describes a syntax for certification request. A certification request consists of a DN, a public key, and additional attributes. Certification requests are sent to a CA, which then issues the certificate.
- **PKCS #11: Cryptographic Token Interface Standard** Specifies an application program interface (API) for token devices that hold encrypted information and perform cryptographic functions, such as smart cards and Universal Serial Bus (USB) pigtails.
- **PKCS #12: Personal Information Exchange Syntax Standard** Specifies a portable format for storing or transporting a user's private keys and certificates. Ties into both PKCS #8 (communication of private-key information) and PKCS #11 (Cryptographic Token Interface Standard). Portable formats include diskettes, smart cards, and Personal Computer Memory Card International Association (PCMCIA) cards. On Microsoft Windows platforms, PKCS #12 format files are generally given the extension .pfx. PKCS #12 is the best standard format to use when exchanging private keys and certificates between systems.



TEST DAY TIP

On the day of the test, do not concern yourself too much with what the different standard numbers are. It is important to understand why they are in place and what PKCS stands for.

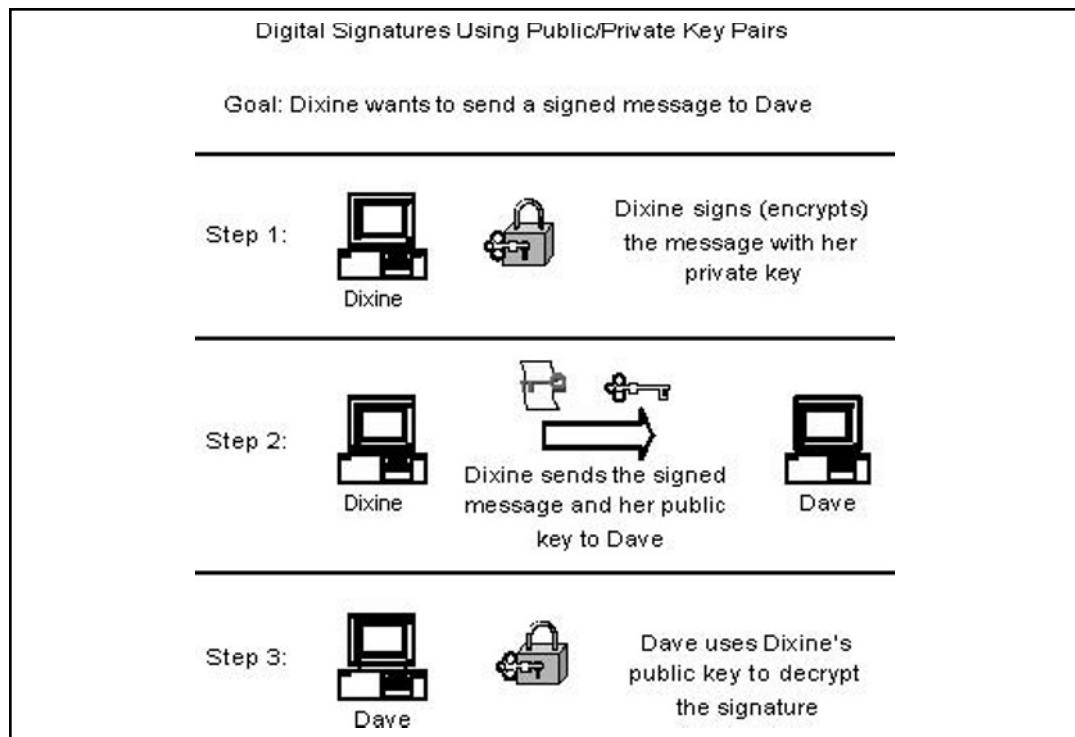
RSA-derived technology in its various forms is used extensively by Windows Server 2008 for such things as Kerberos authentication and S/MIME. In practice, the use of the PKI technology goes something like this: Two users, Dave and Dixine, wish to communicate privately. Dave and Dixine each own a key pair consisting of a public key and a private key. If Dave wants Dixine to send him an encrypted message, he first transmits his public key to Dixine. She then uses Dave's public key to encrypt the message. Fundamentally, since Dave's public key was used to encrypt, only Dave's private key can be used to decrypt. When he receives the message, only he is able to read it. Security is maintained because only public keys are transmitted—the private keys are kept secret and are known only to their owners. Figure 7.1 illustrates the process.

Figure 7.1 Public/Private Key Data Exchange**EXAM WARNING**

In a Windows Server 2008 PKI, a user's public and private keys are stored under the user's profile. For the administrator, the public keys would be under *Documents and Settings\Administrator\System Certificates\My\Certificates* and the private keys would be under *Documents and Settings\Administrator\Crypto\RSA* (where they are double encrypted by Microsoft's Data Protection API, or DPAPI). Although a copy of the public keys is kept in the registry, and can even be kept in Active Directory, the private keys are vulnerable to deletion. If you delete a user profile, the private keys will be lost!

RSA can also be used to create “digital signatures” (see Figure 7.2). In the communication illustrated in Figure 7.1, a public key was used to encrypt a message and the corresponding private key was used to decrypt. If we invert the process, a private key can be used to encrypt and the matching public key to decrypt. This is useful, for example, if you want people to know that a document you wrote is really yours. If you encrypt the document using your private key, then only your public key can decrypt it. If people use your public key to read the document and they are successful, they can be certain that it was “signed” by your private key and is therefore authentic.

Figure 7.2 Digital Signatures



Head of the Class...

Modern Cryptography 101

Thanks to two mathematical concepts, prime number theory and modulo algebra, most of today's cryptography encryption standards are considered intractable—that is, they are unbreakable with current technology in a reasonable amount of time. For example, it might take 300 linked computers over 1,000 years to decrypt a message. Of course, quantum computing is expected to some day change all that, making calculations exponentially faster and rendering all current cryptographic algorithms useless—but we won't worry about that for now.

First, an explanation of the *modulo* operator. Let's go back to elementary school where you first learned to do division. You learned that 19/5 equals 3 with a remainder of 4. You also probably concentrated on the 3 as the important number. Now, however, we get to look at the remainder. When we take the modulus of two numbers, the result is the remainder—therefore $19 \bmod 5$ equals 4. Similarly, $24 \bmod 5$ also equals 4 (can you see why?). Finally, we can conclude that 19 and 24 are congruent in modulo 4. So how does this relate to cryptography and prime numbers?

The idea is to take a message and represent it by using a sequence of numbers. We'll call the sequence x . What we need to do is find three numbers that make the following modulo equation possible: $(x^e)^d \bmod y = x$.

The first two numbers, e and d , are a pair and are completely interchangeable. The third number, y , is a product of two very large prime numbers (the larger the primes, the more secure the encryption). Prime number theory is too complex for an in-depth discussion here, but in a nutshell, remember that a prime number is only divisible by the number 1 and itself. This gives each prime number a "uniqueness."

Once we have found these numbers (although we won't go into how because this is the really deep mathematical part), the encryption key becomes the pair (e, y) and the decryption key becomes the pair (d, y) . Now it doesn't matter which key we decide to make public and which key we make private because they're interchangeable. It's a good thing that Windows Server 2008 does all of the difficult work for us!

How Certificates Work

Before we delve into the inner workings of a certificate, let's discuss what a certificate actually is in layman's terms. In PKI, a digital certificate is a tool used for binding a public key with a particular owner. A great comparison is a driver's license. Consider the information listed on a driver's license:

- Name
- Address
- Date of birth
- Photograph
- Signature
- Social security number (or another unique number such as a state issued license number)
- Expiration date
- Signature/certification by an authority (typically from within the issuing state's government body)

The information on a state license photo is significant because it provides crucial information about the owner of that particular item. The signature from the state official serves as a trusted authority for the state, certifying that the owner has been verified and is legitimate to be behind the wheel of a car. Anyone, like an officer, who wishes to verify a driver's identity and right to commute from one place to another by way of automobile need only ask for and review the driver's license. In some cases, the officer might even call or reference that license number just to ensure it is still valid and has not been revoked.

A digital certificate in PKI serves the same function as a driver's license. Various systems and checkpoints may require verification of the owner's identity and status and will reference the trusted third party for validation. It is the certificate that enables this quick hand-off of key information between the parties involved.

The information contained in the certificate is actually part of the X.509 certificate standard. X.509 is actually an evolution of the X.500 directory standard. Initially intended to provide a means of developing easy-to-use electronic directories of people that would be available to all Internet users, it became a directory and mail standard for a very commonly known mail application: Microsoft Exchange 5.5. The X.500 directory standard specifies a common root of a hierarchical tree although the "tree" is inverted: the root of the tree is depicted at the "top" level while the other

branches—called “containers”—are below it. Several of these types of containers exist with a specific naming convention. In this naming convention, each portion of a name is specified by the abbreviation of the object type or a container it represents. For example, a *CN*= before a username represents it is a “*common name*”, a *C*= precedes a “*country*,” and an *O*= precedes “*organization*”. These elements are worth remembering as they will appear not only in discussions about X.500 and X.509, but they are ultimately the basis for the scheme of Microsoft’s premier directory service, Active Directory.

X.509 is the standard used to define what makes up a digital certificate. Within this standard, a description is given for a certificate as allowing an association between a user’s *distinguished name (DN)* and the user’s public key. The DN is specified by a *naming authority (NA)* and used as a unique name by the *certificate authority (CA)* who will create the certificate. A common X.509 certificate includes the following information (see Table 7.1 and Figures 7.3 and 7.4):

Table 7.1 X.509 Certificate Data

| Item | Definition |
|-----------------------------|--|
| Serial Number | A unique identifier. |
| Subject | The name of the person or company that is being identified, sometimes listed as “Issued To”. |
| Signature Algorithm | The algorithm used to create the signature. |
| Issuer | The trusted authority that verified the information and generated the certificate, sometimes listed as “Issued By”. |
| Valid From | The date the certificate was activated. |
| Valid To | The last day the certificate can be used. |
| Public Key | The public key that corresponds to the private key. |
| Thumbprint Algorithm | The algorithm used to create the unique value of a certificate. |
| Thumbprint | The unique value of every certificate, which positively identifies the certificate. If there is ever a question about the authenticity of a certificate, check this value with the issuer. |

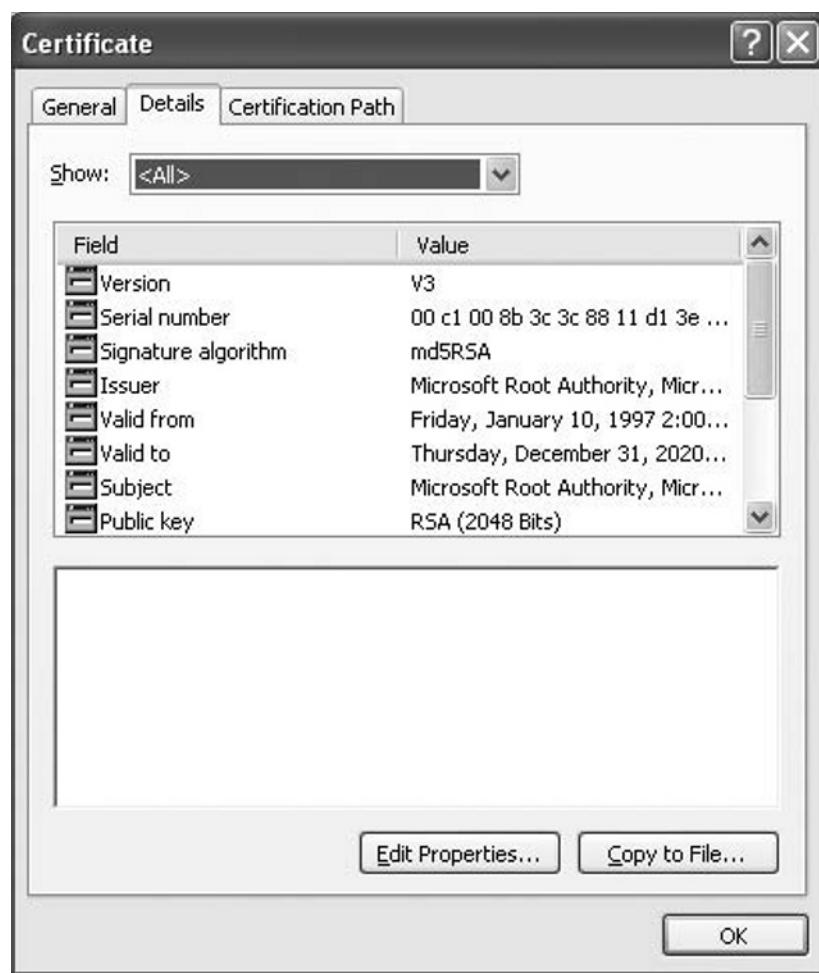
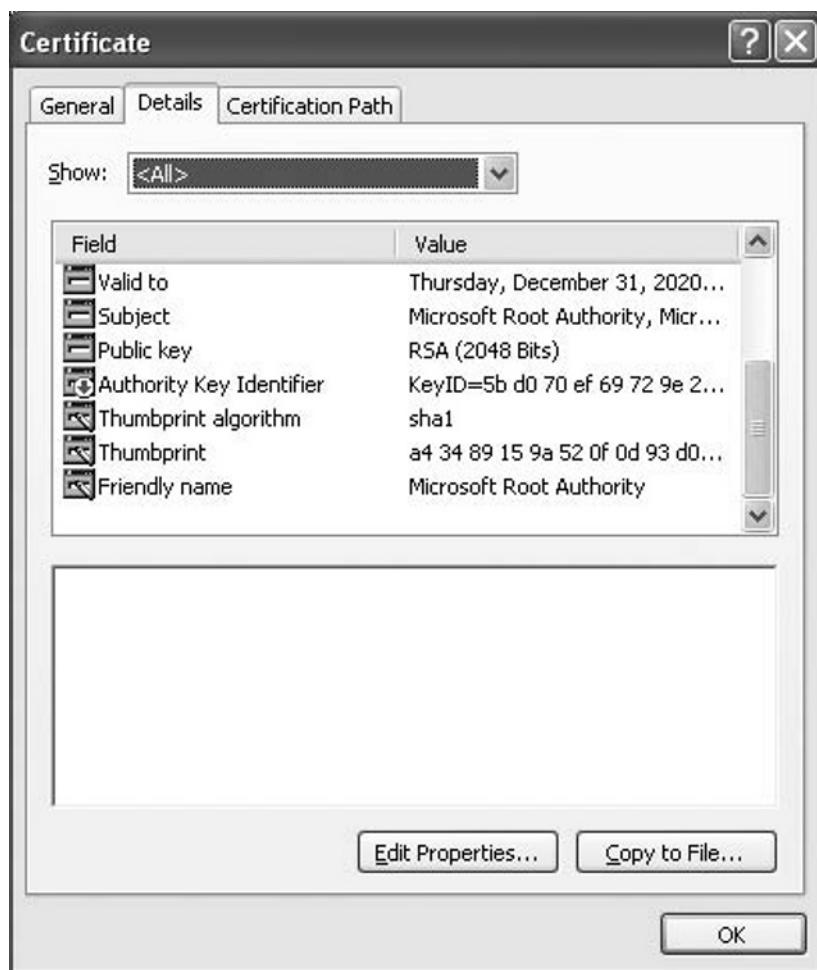
Figure 7.3 A Windows Server 2008 Certificate Field and Values

Figure 7.4 A Windows Server 2008 Certificate Field and Values

Public Key Functionality

Public key cryptography brings major security technologies to the desktop in the Windows 2000 environment. The network now is provided with the ability to allow users to safely:

- Transmit over insecure channels
- Store sensitive information on any commonly used media
- Verify a person's identity for authentication

- Prove that a message was generated by a particular person
- Prove that the received message was not tampered with in transit

Algorithms based on public keys can be used for all these purposes. The most popular public key algorithm is the standard RSA, which is named after its three inventors: Rivest, Shamir, and Adleman. The RSA algorithm is based on two prime numbers with more than 200 digits each. A hacker would have to take the ciphertext and the public key and factor the product of the two primes. As computer processing time increases, the RSA remains secure by increasing the key length, unlike the DES algorithm, which has a fixed key length.

Public key algorithms provide privacy, authentication, and easy key management, but they encrypt and decrypt data slowly because of the intensive computation required. RSA has been evaluated to be from 10 to 10,000 times slower than DES in some environments, which is a good reason not to use public key algorithms for bulk encryption.

Digital Signatures

Document letterhead can be easily created on a computer, so forgery is a security issue. When information is sent electronically, no human contact is involved. The receiver wants to know that the person listed as the sender is really the sender and that the information received has not been modified in any way during transit. A hash algorithm is implemented to guarantee the Windows 2000 user that the data is authentic. A hash value encrypted with a private key is called a digital signature. Anyone with access to the corresponding public key can verify the authenticity of a digital signature. Only a person having a private key can generate digital signatures. Any modification makes a digital signature invalid.

The purpose of a digital signature is to prevent changes within a document from going unnoticed and also to claim the person to be the original author. The document itself is not encrypted. The digital signature is just data sent along with the data guaranteed to be untampered with. A change of any size invalidates the digital signature.

When King Henry II had to send a message to his troops in a remote location, the letter would be sealed with wax, and while the wax was still soft the king would use his ring to make an impression in it. No modification occurred to the original message if the seal was never broken during transit. There was no doubt that King Henry II had initiated the message, because he was the only person possessing a ring that matched the waxed imprint. Digital signatures work in a similar fashion in that only the sender's public key can authenticate both the original sender and the content of the document.

The digital signature is generated by a message digest, which is a number generated by taking the message and using a hash algorithm. A message digest is regarded as a fingerprint and can range from a 128-bit number to a 256-bit number. A hash function takes variable-length input and produces a fixed-length output. The message is first processed with a hash function to produce a message digest. This value is then signed by the sender's private key, which produces the actual digital signature. The digital signature is then added to the end of the document and sent to the receiver along with the document.

Since the mere presence of a digital signature proves nothing, verification must be mathematically proven. In the verification process, the first step is to use the corresponding public key to decrypt the digital signature. The result will produce a 128-bit number. The original message will be processed with the same hash function used earlier and will result in a message digest. The two resulting 128-bit numbers will then be compared, and if they are equal, you will receive notification of a good signature. If a single character has been altered, the two 128-bit numbers will be different, indicating that a change has been made to the document, which was never scrambled.

Authentication

Public key cryptography can provide authentication instead of privacy. In Windows 2000, a challenge is sent by the receiver of the information. The challenge can be implemented one of two ways. The information is authenticated because only the corresponding private key could have encrypted the information that the public key is successfully decrypting.

In the first authentication method, a challenge to authenticate involves sending an encrypted challenge to the sender. The challenge is encrypted by the receiver, using the sender's public key. Only the corresponding private key can successfully decode the challenge. When the challenge is decoded, the sender sends the plaintext back to the receiver. This is the proof for the receiver that the sender is truly the sender.

For example, when Alice receives a document from Bob, she wants to authenticate that the sender is really Bob. She sends an encrypted challenge to Bob, using his public key. When he receives the challenge, Bob uses his private key to decrypt the information. The decrypted challenge is then sent back to Alice. When Alice receives the decrypted challenge, she is convinced that the document she received is truly from Bob.

The second authentication method uses a challenge that is sent in plaintext. The receiver, after receiving the document, sends a challenge in plaintext to the

sender. The sender receives the plaintext challenge and adds some information before adding a digital signature.

The challenge and digital signature now head back to the sender. The digital signature is generated by using a hash function and then encrypting the result with a private key, so the receiver must use the sender's public key to verify the digital signature. If the signature is good, the original document and sender have at this point been verified mathematically.

Secret Key Agreement via Public Key

The PKI of Windows 2000 permits two parties to agree on a secret key while they use nonsecure communication channels. Each party generates half the shared secret key by generating a random number, which is sent to the other party after being encrypted with the other party's public key. Each receiving side then decrypts the ciphertext using a private key, which will result in the missing half of the secret key.

By adding both random numbers together, each party will have an agreed-upon shared secret key, which can then be used for secure communication even though the secret key was first obtained through a nonsecure communication channel.

Bulk Data Encryption without Prior Shared Secrets

The final major feature of public key technology is that it can encrypt bulk data without generating a shared secret key first. The biggest disadvantage of using asymmetric algorithms for encryption is the slowness of the overall process, which results from the necessary intense computations; the largest disadvantage of using symmetric algorithms for encryption of bulk data is the need for a secure communication channel for exchanging the secret key. The Windows 2000 operating system combines symmetric and asymmetric algorithms to get the best of both worlds at just the right moment.

For a large document that must be kept secret, because secret key encryption is the quickest method to use for bulk data, a session key is used to scramble the document. To protect the session key, which is the secret key needed to decrypt the protected data, the sender encrypts this small item quickly by using the receiver's public key. This encryption of the session key is handled by asymmetric algorithms, which use intense computation, but do not require much time due to the small size of the session key. The document, along with the encrypted session key, is then sent to the receiver. Only the intended receiver will possess the correct private key to decode the session key, which is needed to decode the actual document. When the session key is in plaintext, it can be applied to the ciphertext of the bulk data and then transform the bulk data back to plaintext.

EXERCISE 7.1

REVIEWING A DIGITAL CERTIFICATE

Let's take a moment to go on the Internet and look at a digital certificate.

1. Open up your Web browser, and go to www.syngress.com.
2. Select a book and add it to your cart.
3. Proceed to the checkout.
4. Once you are at the checkout screen, you will see a padlock in your browser. In Internet Explorer 7, this will be to the right of the address box; older browsers place the padlock in the bottom right of the window frame. Open the certificate properties. In Internet Explorer 7, you do this by clicking on the padlock and selecting "View Certificates" from the prompt; older browsers generally let you double-click the padlock.
5. Move around the tabs of the Properties screen to look at the different information contained within that certificate.

The Windows Server 2008 PKI does many things behind the scenes. Thanks in part to auto enrollment (discussed later in this chapter) and certificate stores (places where certificates are kept after their creation), some PKI-enabled features such as EFS work with no user intervention at all. Others, such as IPsec, require significantly less work than would be required without an advanced operating system.

Even though a majority of the PKI is handled by Server, it is still instructive to have an overview of how certificate services work.

1. First, a system or user generates a public/private key pair and then a certificate request.
2. The certificate request, which contains the public key and other identifying information such as user name, is forwarded on to a CA.
3. The CA verifies the validity of the public key. If it is verified, the CA issues the certificate.
4. Once issued, the certificate is ready for use and is kept in the certificate store, which can reside in Active Directory. Applications that require a certificate use this central repository when necessary.

In practice, it isn't terribly difficult to implement certificate services, as Exercise 7.2 shows. Configuring the CA requires a bit more effort, as does planning the structure

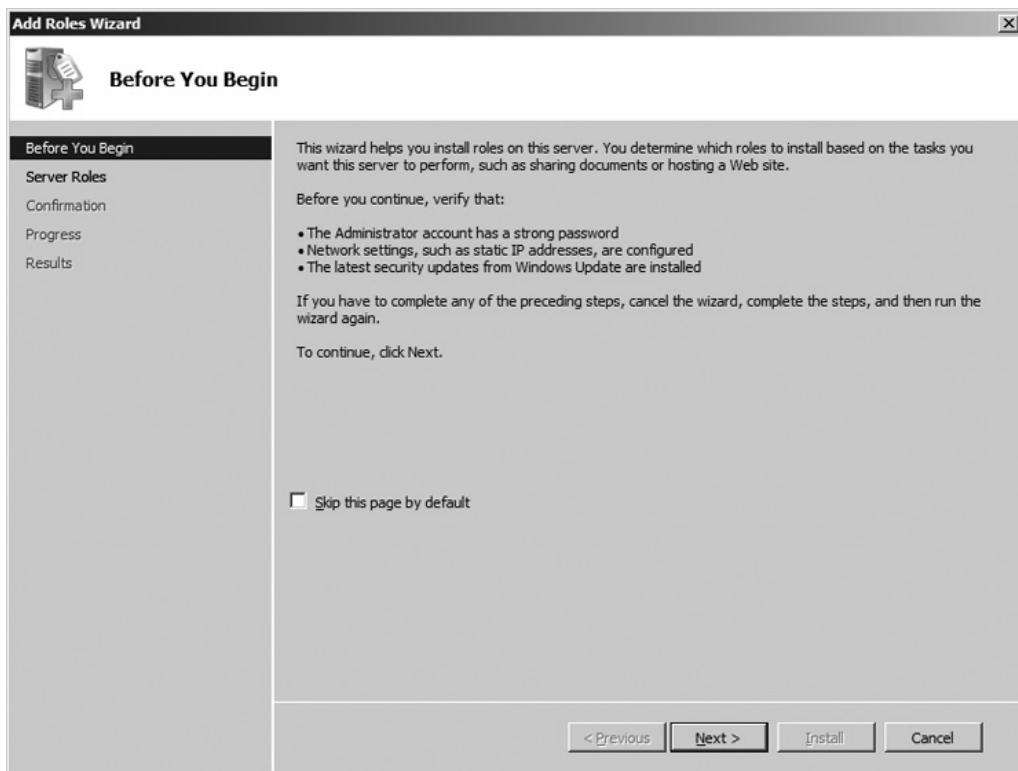
and hierarchy of the PKI—especially if you are designing an enterprise-wide solution. We'll cover these topics later in this chapter.

EXERCISE 7.2

INSTALLING CERTIFICATE SERVICES

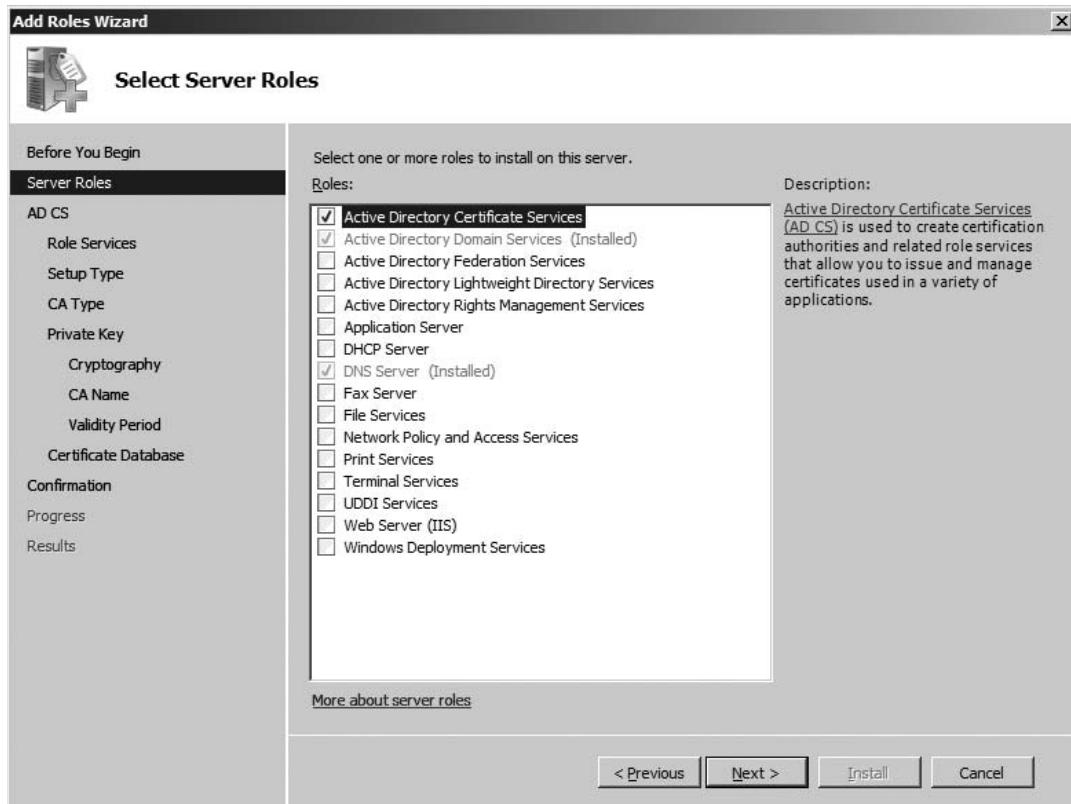
1. After logging on with administrative privileges, click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Server Manager**.
2. In the **Roles Summary** section, click **Add Roles**.
3. On the **Before You Begin** page, click **Next** (see Figure 7.5).

Figure 7.5 Before You Begin Page

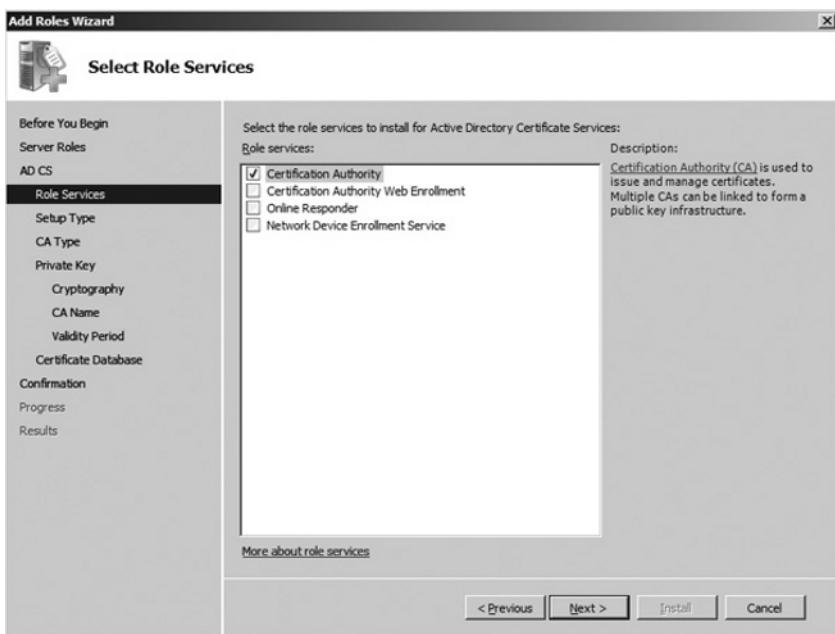


4. On the **Select Server Roles** page, click the **Active Directory Certificate Services** (see Figure 7.6). Click **Next**.

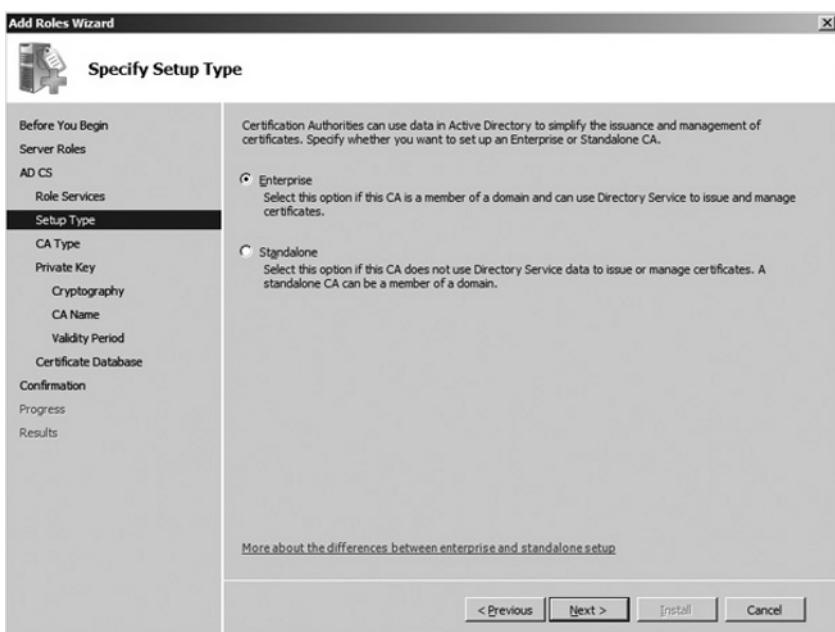
Figure 7.6 Select Server Roles Page



5. On the **Introduction to Active Directory Certificate Services** page, click **Next**.
6. On the **Select Role Services** page, click the **Certification Authority** check box, as shown in Figure 7.7. Click **Next**.

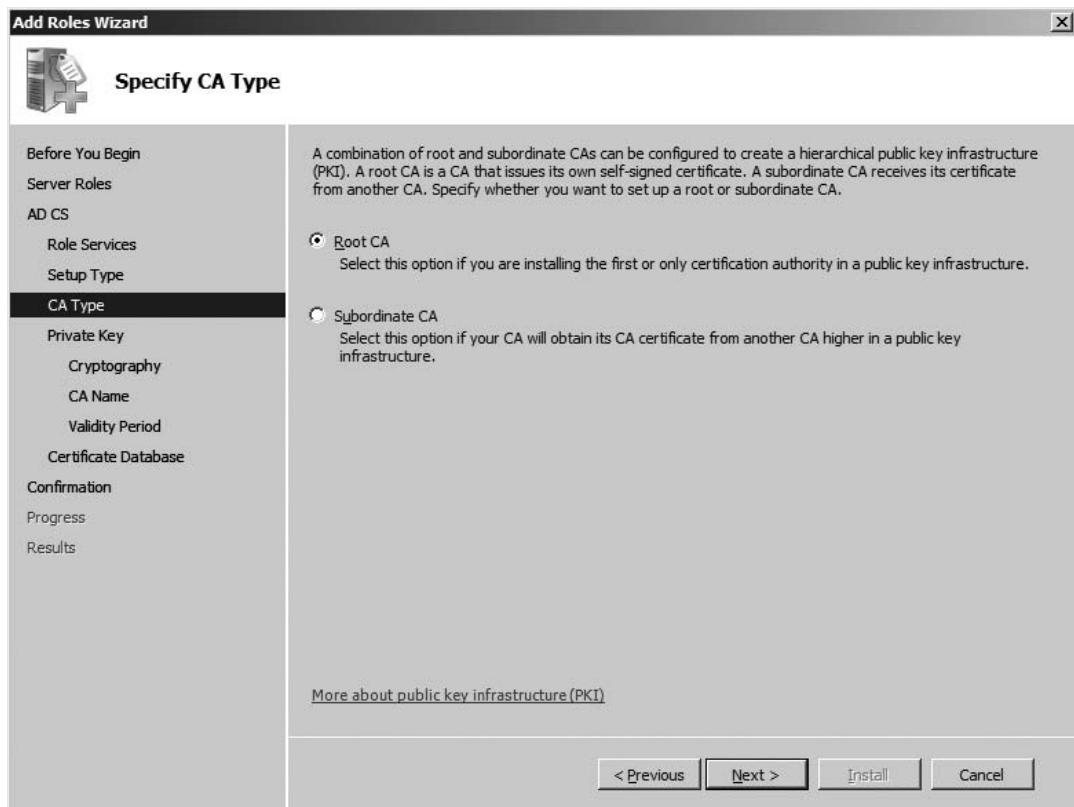
Figure 7.7 Select Role Services Page

7. On the **Specify Setup Type** page, click **Enterprise**, as shown in Figure 7.8. Click **Next**.

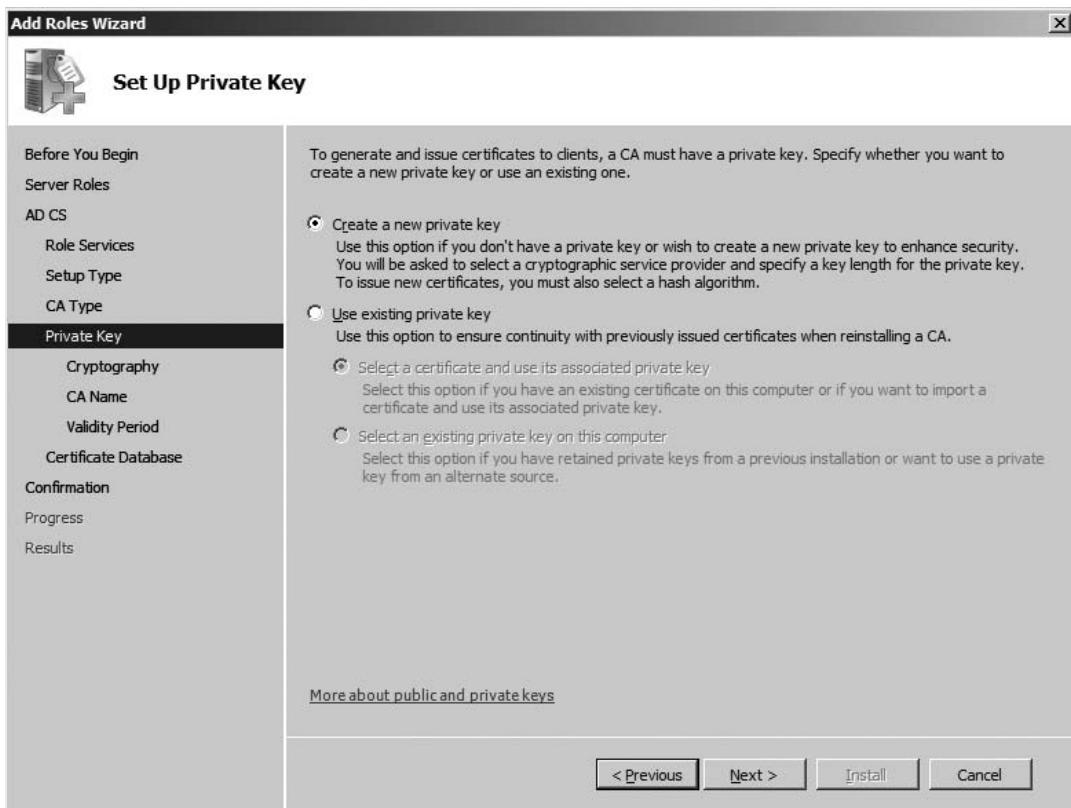
Figure 7.8 Specify Setup Type Page

8. On the **Specify CA Type** page, click **Root CA**, as shown in Figure 7.9. Click **Next**.

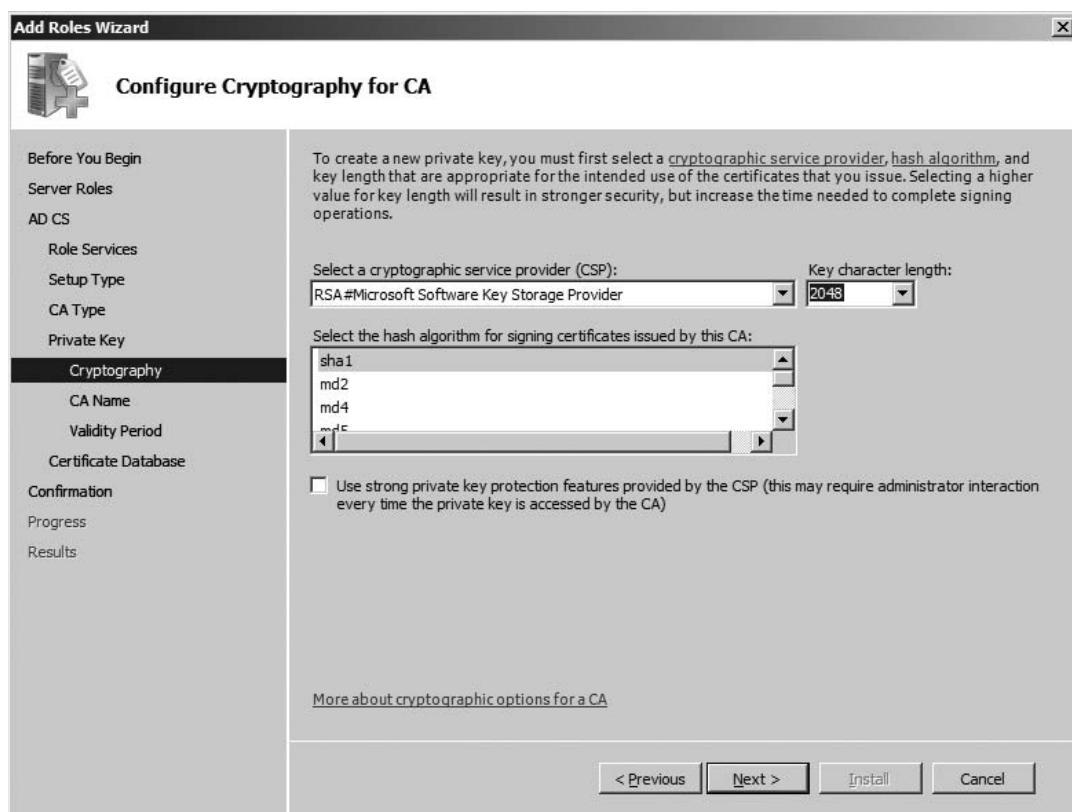
Figure 7.9 Specify CA Type Page



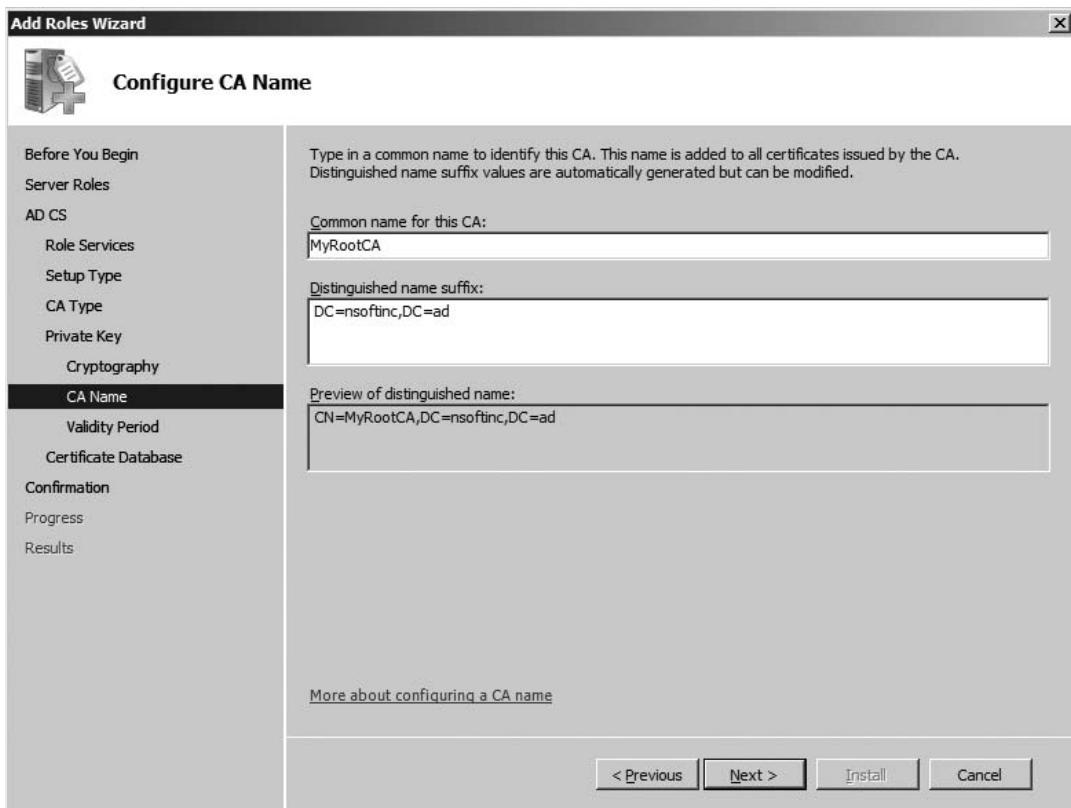
9. On the **Set Up Private Key** page, either accept the default value or configure optional configuration settings. For this exercise, choose the default settings as shown in Figure 7.10. Click **Next**.

Figure 7.10 Set Up Private Key Page

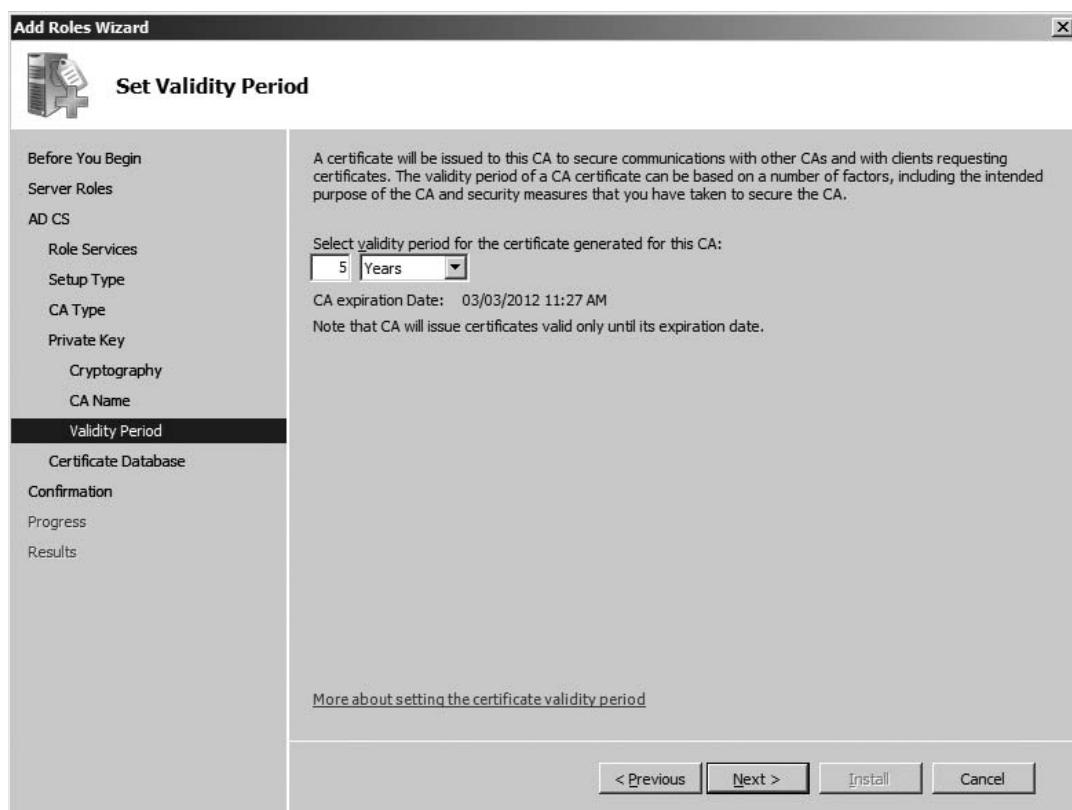
10. On the **Configure Cryptography for CA** page, either accept the default value or configure optional configuration settings as per project requirements. For this exercise, choose the default settings as shown in Figure 7.11. Click **Next**.

Figure 7.11 Configure Cryptography for CA Page

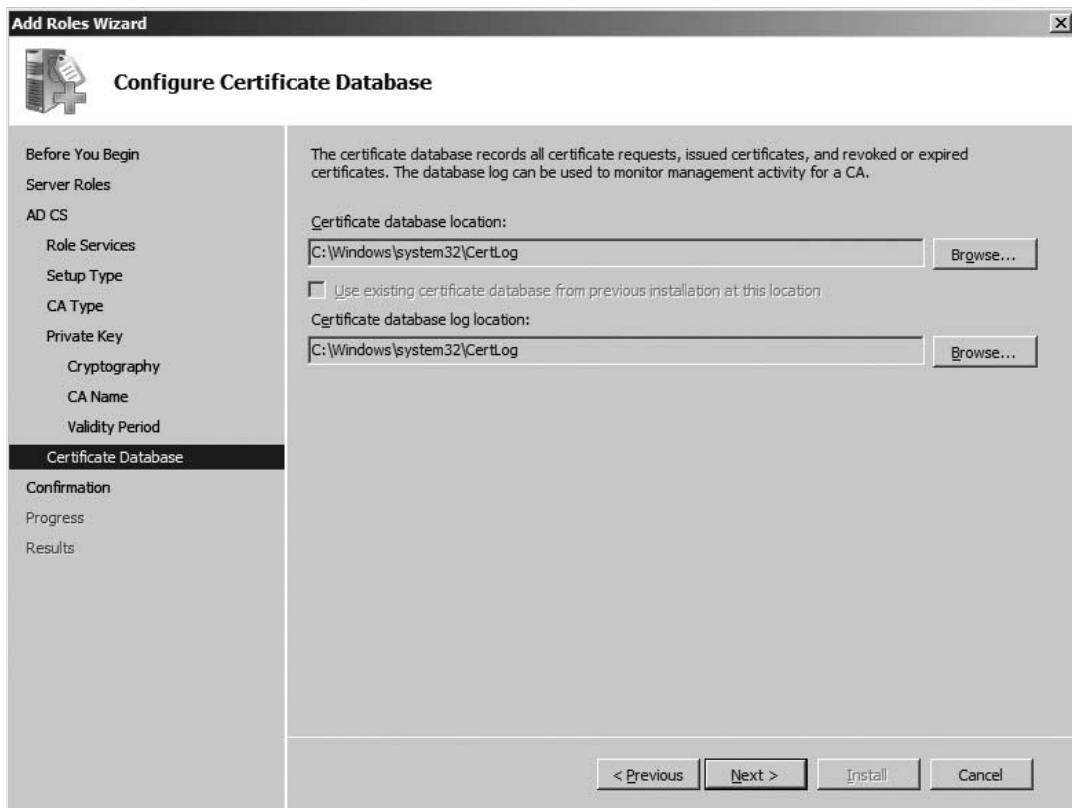
11. In the **Common name for this CA** box, type the common name of the CA. For this exercise, type **MyRootCA** as shown in Figure 7.12. Click **Next**.

Figure 7.12 Configure CA Name Page

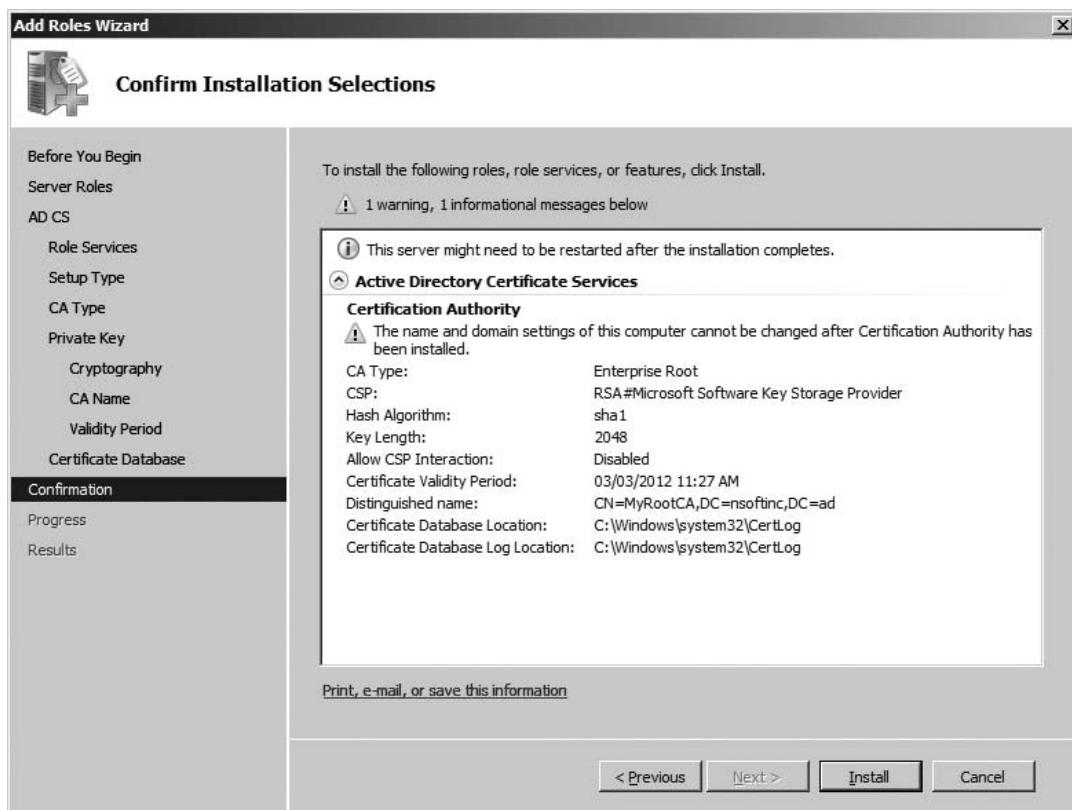
12. On the **Set the Certificate Validity Period** page, you can change the default five-year validity period of the CA. You can set the validity period as a number of days, weeks, months or years. Accept the default validity duration for the root CA as shown in Figure 7.13, and then click **Next**.

Figure 7.13 Set Validity Period Page

14. On the **Configure Certificate Database** page, for this exercise, accept the default values or specify other storage locations for the certificate database and the certificate database log (see Figure 7.14). Click **Next**.

Figure 7.14 Configure Certificate Database Page

15. On the **Confirm Installation Selections** page, click **Install** (see Figure 7.15).

Figure 7.15 Confirm Installation Selections Page

16. On the Installation Results page, review the information and make sure it read **Installation succeeded**.
17. Click **Close** to close the Add Roles Wizard.



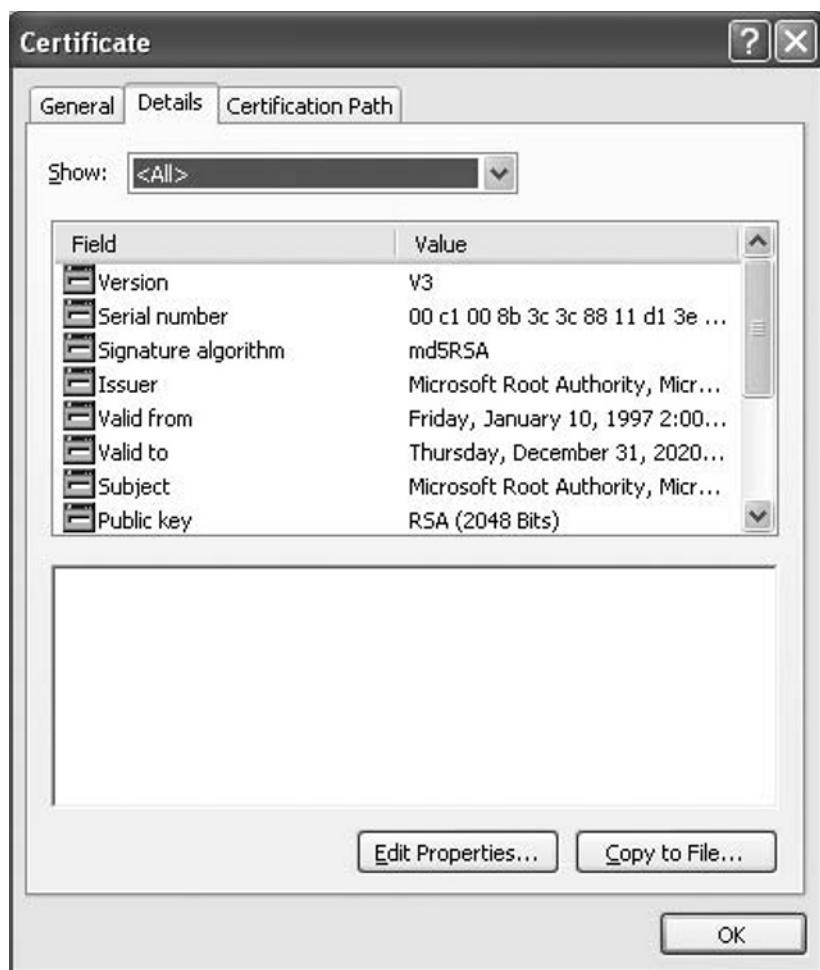
TEST DAY TIP

Pay special attention to the above exercise as you may be asked questions about the distinguished name of the CA.

In our previous discussion of public and private key pairs, two users wanted to exchange confidential information and did so by having one user encrypt the data with the other user's public key. We then discussed digital signatures, where the sending user "signs" the data by using his or her private key. Did you notice the security vulnerability in these methods?

In this type of scenario, there is nothing to prevent an attacker from intercepting the data mid-stream, and replacing the original signature with his or her own, using of course his or her own private key. The attacker would then forward the replacement public key to the unsuspecting party. In other words, even though the data is signed, how can you be sure of who signed it? The answer in the Windows PKI is the certificate.

Think of a certificate as a small and portable combination safe. The primary purpose of the safe is to hold a public key (although quite a bit of other information is also held there). The combination to the safe must be held by someone you trust—that trust is the basis for the entire PKI system. If I am a user and want to send you my public key so that you can encrypt some data to send back to me, I can just sign the data myself, but I am then vulnerable to the attack mentioned above. However if I allow a trusted third party entity to take my public key (which I don't mind because they're trustworthy), lock it away in the safe and then send the safe to you, you can ask the trusted party for the combination. When you open the safe, you can be certain that the public key and all other information inside really belongs to me, because the safe came from a trustworthy source. The "safe" is really nothing more than a digital signature, except that the signature comes from a universally trusted third party and not from me. The main purpose of certificates, then, is to facilitate the secure transfer of keys across an insecure network. Figure 7.16 shows the properties of a Windows certificate—notice that the highlighted public key is only part of the certificate.

Figure 7.16 A Windows Server 2008 Certificate

User Certificates

Of the three general types of certificates found in a Windows PKI, the *user certificate* is perhaps the most common. User certificates are certificates that enable the user to do something that would not be otherwise allowed. The Enrollment Agent certificate is one example. Without it, even an administrator is not able to enroll smart cards and configure them properly at an enrollment station. Under Windows Server 2008, required user certificates can be requested automatically by the client and subsequently issued by a certification authority (discussed below) with no user intervention necessary.

Machine Certificates

Also known as computer certificates, *machine certificates* (as the name implies) give the system—instead of the user—the ability to do something out of the ordinary. The main purpose for machine certificates is authentication, both client-side and server-side. As stated earlier, certificates are the main vehicle by which public keys are exchanged in a PKI. Machine certificates are mainly involved with these behind-the-scenes exchanges, and are normally overseen by the operating system. Machine certificates have been able to take advantage of Windows' autoenrollment feature since 2000 Server was introduced. We will discuss auto-enrollment later in this chapter.

Application Certificates

The term *application certificate* refers to any certificate that is used with a specific PKI-enabled application. Examples include IPsec and S/MIME encryption for e-mail. Applications that need certificates are generally configured to automatically request them, and are then placed in a waiting status until the required certificate arrives. Depending upon the application, the network administrator or even the user might have the ability to change or even delete certificate requests issued by the application.



TEST DAY TIP

Certificates are at the very core of the Windows PKI. Make certain that you understand what certificates are, and why they are needed when using public keys. Also, be familiar with the types of certificates listed in this section and the differences between them.

Analyzing Certificate Needs within the Organization

We've just concluded a tour of most of the properties associated with a CA, but knowing what you *can* do does not mean that we know what you *should* do. To find out more about what you should do, you need to analyze the certificate needs of your organization, and then move on to create an appropriate CA structure.

According to Microsoft's TechNet, the analysis of certificate needs springs primarily from “the analysis of business requirements and the analysis of applications that benefit from PKI-based security”. In other words, when designing a PKI/CA

structure, you will need to understand the different uses for certificates and whether your organization needs to use certificates for each of these purposes. Examples include SSL for a secure Web server, EFS for encryption of files, and S/MIME for encryption of e-mail messages. The use of S/MIME might dictate that your CA hierarchy have a trust relationship with external CAs, and the use of SSL might lead you to implement a stand-alone CA instead of an enterprise CA. Thus, analyzing these needs *before* you implement your PKI can save you a lot of time and trouble.

Working with Certificate Services

Certificate Services in Windows Server 2008 is an easier venture than ever before. As we look at what is entailed in the components involved in establishing and supporting a PKI in Windows Server 2008 we need to quickly discuss what Certificate Services do for us.

In Active Directory and Windows Server 2008, Certificate Services allow administrators to establish and manage the PKI environment. More generally, they allow for a trust model to be established within a given organization. The trust model is the framework that will hold all the pieces and components of the PKI in place. Typically, there are two options for a trust model within PKI: a *single CA model* and a *hierarchical model*. The certificate services within Windows Server 2008 provide the interfaces and underlying technology to setup and manage both of these type of deployments.

Configuring a Certificate Authority

By definition, a certificate authority is an entity (computer or system) that issues digital certificates of authenticity for use by other parties. With the ever increasing demand for effective and efficient methods to verify and secure communications, our technology market has seen the rise of many trusted third parties into the market. If you have been in the technology field for any length of time, you are likely familiar with many such vendors by name: VeriSign, Entrust, Thawte, GeoTrust, DigiCert and GoDaddy are just a few.

While these companies provide an excellent and useful resource for both the IT administrator and the consumer, companies and organizations desired a way to establish their own certificate authorities. In a third-party, or external PKI, it is up to the third-party CA to positively verify the identity of anyone requesting a certificate from it. Beginning with Windows 2000, Microsoft has allowed the creation of a trusted *internal* CA—possibly eliminating the need for an external third party. With a Windows Server 2008 CA, the CA verifies the identity of the

user requesting a certificate by checking that user's authentication credentials (using Kerberos or NTLM). If the credentials of the requesting user check out, a certificate is issued to the user. When the user needs to transmit his or her public key to another user or application, the certificate is then used to prove to the receiver that the public key inside can be used safely.

Certificate Authorities

Certificates are a way to transfer keys securely across an insecure network. If any arbitrary user were allowed to issue certificates, it would be no different than that user simply signing the data. In order for a certificate to be of any use, it must be issued by a trusted entity—an entity that both the sender and receiver trust. Such a trusted entity is known as a *Certification Authority* (CA). Third-party CAs such as VeriSign or Entrust can be trusted because they are highly visible, and their public keys are well known to the IT community. When you are confident that you hold a true public key for a CA, and that public key properly decrypts a certificate, you are then certain that the certificate was digitally signed by the CA and no one else. Only then can you be positive that the public key contained inside the certificate is valid and safe.

In the analogy we used earlier, the state driver's licensing agency is trusted because it is known that the agency requires proof of identity before issuing a driver's license. In the same way, users can trust the certification authority because they know it verifies the authentication credentials before issuing a certificate. Within an organization leveraging Windows Server 2008, several options exist for building this trust relationship. Each of these begins with the decisions made around selecting and implementing certificate authorities. With regard to the Microsoft implementation of PKI, there are at least four major roles or types of certificate authorities to be aware of:

- Enterprise CA
- Standard CA
- Root CA
- Subordinate CA

Believe it or not, beyond this list at least two variations exist: intermediate CAs and leaf CAs, each of which is a type of subordinate CA implementation.

Standard vs. Enterprise

An enterprise CA is tied into Active Directory and is required to use it. In fact, a copy of its own CA certificate is stored in Active Directory. Perhaps the biggest

difference between an enterprise CA and a stand-alone CA is that enterprise CAs use Kerberos or NTLM authentication to validate users and computers before certificates are issued. This provides additional security to the PKI because the validation process relies on the strength of the Kerberos protocol, and not a human administrator. Enterprise CAs also use templates, which are described later in this chapter, and they can issue every type of certificate.

There are also several downsides to an enterprise CA. In comparison to a stand-alone CA, enterprise CAs are more difficult to maintain and require a much more in-depth knowledge about Active Directory and authentication. Also, because an enterprise CA requires Active Directory, it is nearly impossible to remove it from the network. If you were to do so, the Directory itself would quickly become outdated—making it difficult to resynchronize with the rest of the network when brought back online. Such a situation would force an enterprise CA to remain attached to the network, leaving it vulnerable to attackers.

Root vs. Subordinate Certificate Authorities

As discussed earlier, there are two ways to view PKI trust models: single CA and hierarchical. In a single CA model PKIs are very simplistic; only one CA is used within the infrastructure. Anyone who needs to trust parties vouched for by the CA is given the public key for the CA. That single CA is responsible for the interactions that ensue when parties request and seek to verify the information for a given certificate.

In a hierarchical model, a root CA functions as a top-level authority over one or more levels of CAs beneath it. The CAs below the root CA are called subordinate CAs. Root CAs serve as a *trust anchor* to all the CA's beneath it and to the users who trust the root CA. A trust anchor is an entity known to be trusted without requiring that it be trusted by going to another party, and therefore can be used as a base for trusting other parties. Since there is nothing above the root CA, no one can vouch for its identity; it must create a *self-signed* certificate to vouch for itself. With a self-signed certificate, both the certificate issuer and the certificate subject are exactly the same. Being the trust anchor, the root CA must make its own certificate available to all of the users (including subordinate CAs) that will ultimately be using that particular root CA.

Hierarchical models work well in larger hierarchical environments, such as large government organizations or corporate environments. Often, a large organization also deploys a Registration Authority (RA, covered later in this chapter), Directory Services and optionally Timestamping Services in an organization leveraging a hierarchical approach to PKI. In situations where different organization are trying to develop a

hierarchical model together (such as post acquisition or merger companies or those that are partnered for collaboration), a hierarchical model can be very difficult to establish as both parties must ultimately agree upon a single trust anchor.

When you first set up an internal PKI, no CA exists. The first CA created is known as the root CA, and it can be used to issue certificates to users or to other CAs. As mentioned above, in a large organization there usually is a hierarchy where the root CA is not the only certification authority. In this case, the sole purpose of the root CA is to issue certificates to other CAs in order to establish their authority.

Any certification authority that is established after the root CA is a subordinate CA. Subordinate CAs gain their authority by requesting a certificate from either the root CA or a higher level subordinate CA. Once the subordinate CA receives the certificate, it can control CA policies and/or issue certificates itself, depending on your PKI structure and policies.

Sometimes, subordinate CAs also issue certificates to other CAs below them on the tree. These CAs are called *intermediate CAs*. In most hierarchies, there is more than one intermediate CA. Subordinate CAs that issue certificates to end users, server, and other entities but do not issue certificates to other CAs are called *leaf CAs*.

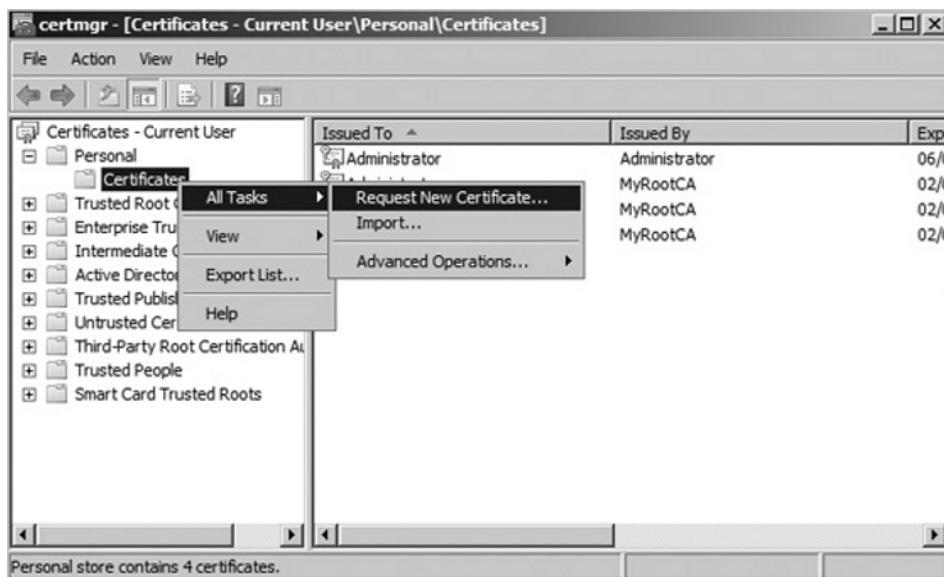
Certificate Requests

In order to receive a certificate from a valid issuing CA, a client—computer or user—must request a certificate from a CA.

There are three ways that this request can be made:

- Autoenrollment
- Use of the Certificates snap-in
- Via a web browser

It is very likely that the most common method for requesting a certificate is autoenrollment, and we'll discuss its deployment shortly. A client can also request a certificate by use of the **Certificates** snap-in. The snap-in, shown in Figure 7.17, can be launched by clicking **Start | Run**, and then typing in **certmgr.msc** and pressing **Enter**. Note that the **Certificates** snap-in does *not* appear in the **Administrative Tools** folder as the **Certification Authority** snap-in does after installing certificate services. Once you open the Certificate Snap-in, expand the **Personal** container, and then right-clicking the **Certificates** container beneath it. You can start the **Certificate Request Wizard** by choosing **All Tasks | Request New Certificate...**, as shown in the following figure:

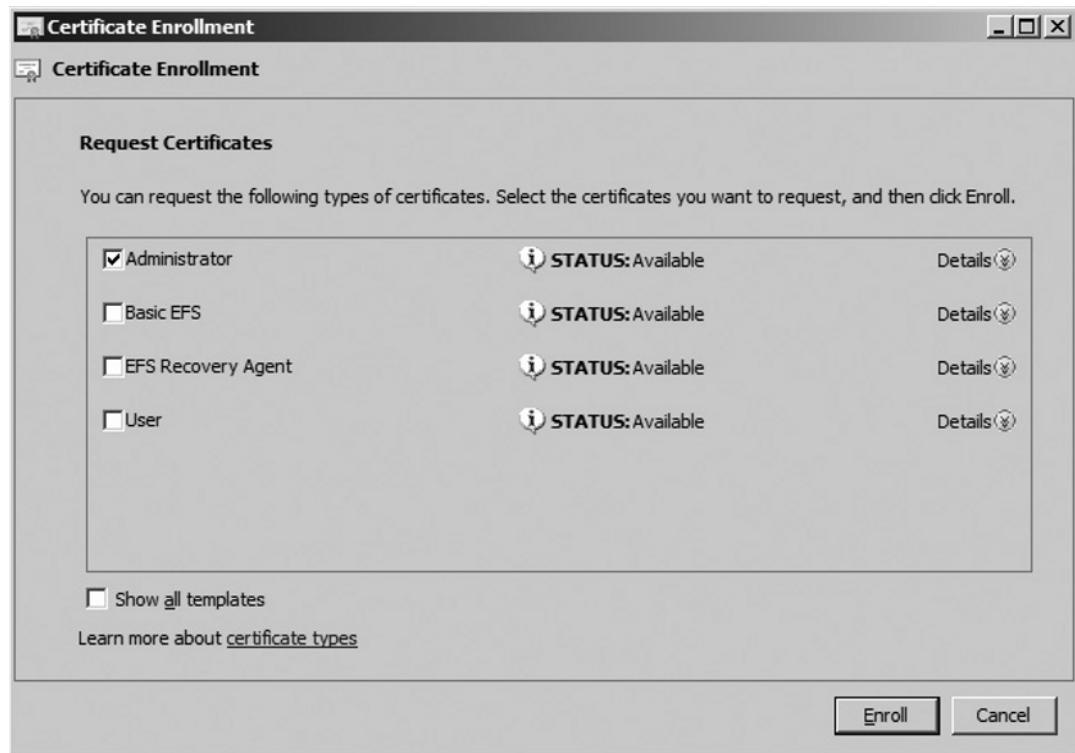
Figure 7.17 Certificates Snap-in

Next, you will receive the **Before You Begin** welcome screen, as shown in Figure 7.18. Click **Next**.

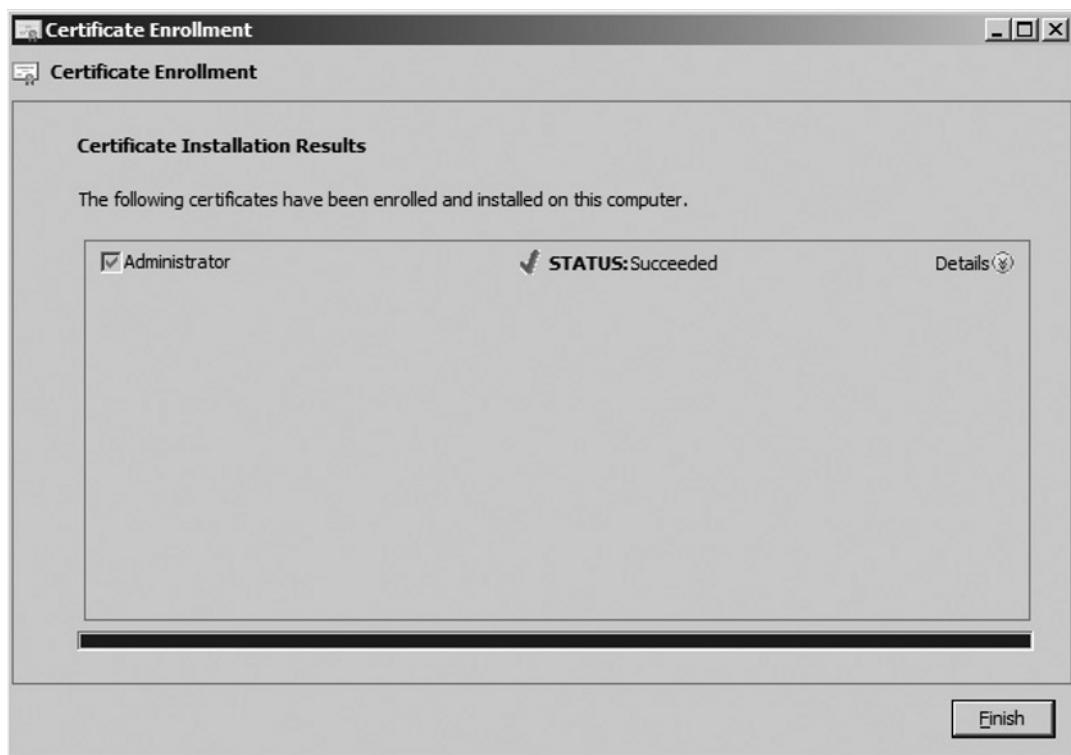
Figure 7.18 Before You Begin

Next to Welcome screen, the wizard prompts you to choose the certificate enrollment type. Figure 7.19 shows you the available options. You can choose only a type for which the receiving CA has a template. Once you choose an appropriate template, click **Enroll**.

Figure 7.19 Request Certificates



Next to Certificate Enrollment screen, verify it reads, STATUS: Succeeded, as shown in Figure 7.20. Click **Finish** to complete the request.

Figure 7.20 Certificate Installation Results

The last method for requesting a certificate is to use a Web browser on the client machine. Note that if you use this option, IIS must be installed on the CA. Exercise 7.3 shows the steps for requesting a certificate using a client machine in this manner.

TEST DAY TIP

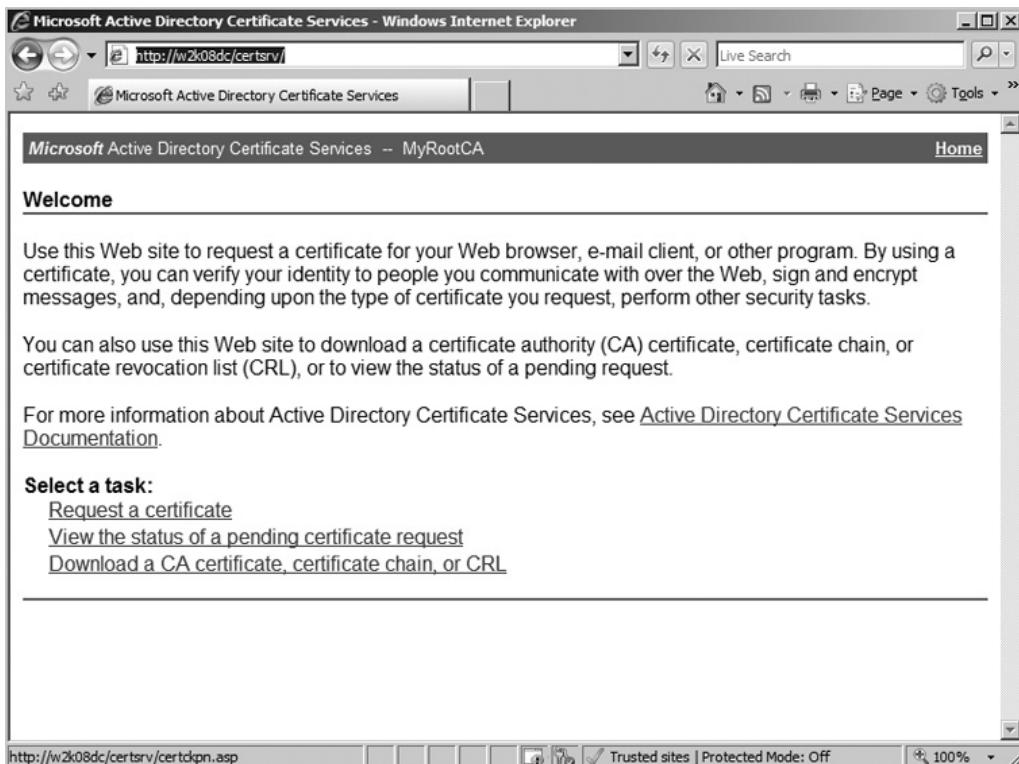
The order of component installation can be important when dealing with CAs. If you install certificate services *before* you install IIS, a client will *not* be able to connect as in the exercise below until you run the following from the command line: `certutil -vroot`. This establishes the virtual root directories necessary for Web enrollment. Note also that you must have selected the Web enrollment support option during the certificate services installation procedure that we completed in Exercise 7.1.

EXERCISE 7.3

REQUEST A CERTIFICATE FROM A WEB SERVER

1. On any computer for which you want to request a certificate, launch Internet Explorer (version 5.0 or later) by clicking **Start | Programs or All Programs | Internet Explorer**.
2. In the address bar, type **http://servername/certsrv**, where servername is the name of the issuing CA.
3. When the welcome screen appears, as shown in Figure 7.21, click **Request a Certificate**.

Figure 7.21 Welcome Screen of the CA's Web Site



4. Click **User Certificate**, then **Submit** when the next screen appears.
5. When the **Certificate Issued** page appears, click **Install This Certificate**. Close the browser.

Certificate Practice Statement

As the use of X.509-based certificates continues to grow it becomes increasingly important that the management of an organization of certificates be as diligent as possible. We know what a digital certificate is and what its critical components are, but a CA can issue a certificate for a number of different reasons. The certificate, then, must indicate exactly what the certificate will be used for. The set of rules that indicates exactly how a certificate may be used (what purpose it can be trusted for, or perhaps the community for which it can be trusted) is called a certificate policy. The X.509 standard defines certificate policies as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.”

Different entities have different security requirements. For example, users want a digital certificate for securing e-mail (either encrypting the incoming messages signing outgoing mail), Syngress (as other Web vendors do) wants a digital certificate for their online store, etc. Every user will want to secure their information, and a certificate owner will use the policy information to determine if they want to accept a certificate.

It is important to have a policy in place to state what the appropriate protocol is for use of certificates—how they are requested, how and when they may be used, etc.—but it is equally as important to explain exactly how to implement those policies. This is where the Certificate Practice Statement (CPS) comes in. A CPS describes how the CA plans to manage the certificates it issues.

Key Recovery

Key recovery is compatible with the CryptoAPI architecture of Windows 2008, but it is not a necessary requirement. For key recovery, an entity’s private key must be stored permanently. The storage of private keys guarantees that critical information will always be accessible, even if the information should get corrupted or deleted. On the other hand, there is a security issue in the backup of the private keys. The archived private key should be used to impersonate the private key owner only if corruption occurs on your system.

Backup and Restore

Microsoft recommends that you back up your entire CA server. By backing up the system state data on your CA, you will automatically get a backup of the certificate store, the registry, system files, and Active Directory (if your CA is a domain controller). Sometimes, you may want to just back up the certificate services portion of your computer without doing a full backup of everything else.

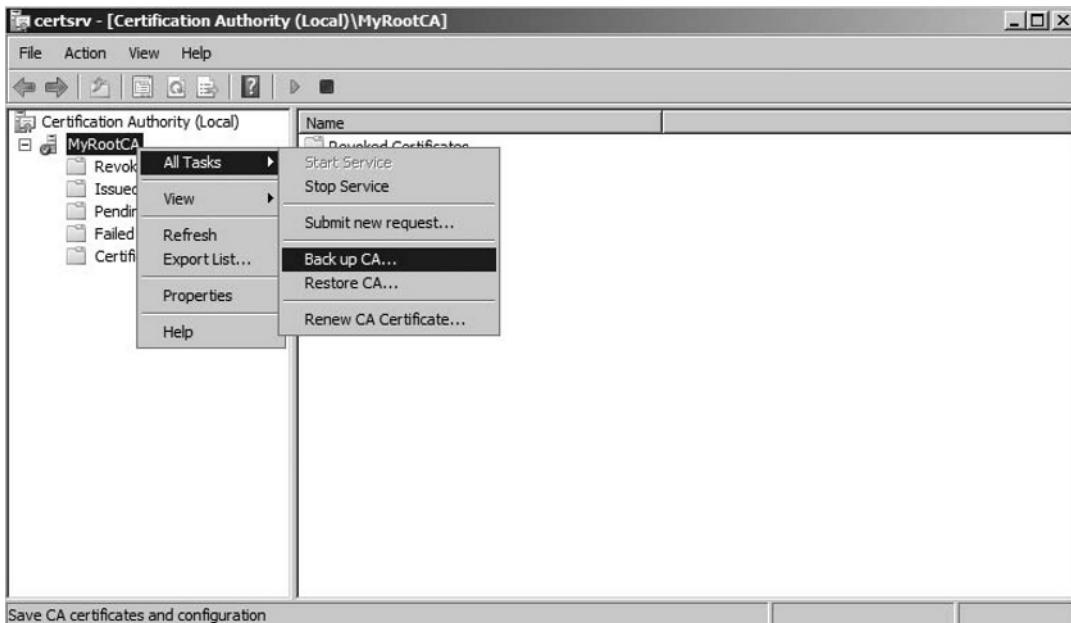
Exercise 7.4 walks you through backing up Certificate Services. Your backups are only useful if you can restore them—Exercise 7.5 walks you through restoring Certificate Services.

EXERCISE 7.4

BACKING UP CERTIFICATE SERVICES

1. On any computer for which you want to take a backup, Log on with administrative privileges.
2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Certification Authority**.
3. Right-click the name of your CA, and choose **All Tasks | Back up CA...** from the pop-up menu, as shown in Figure 7.22.

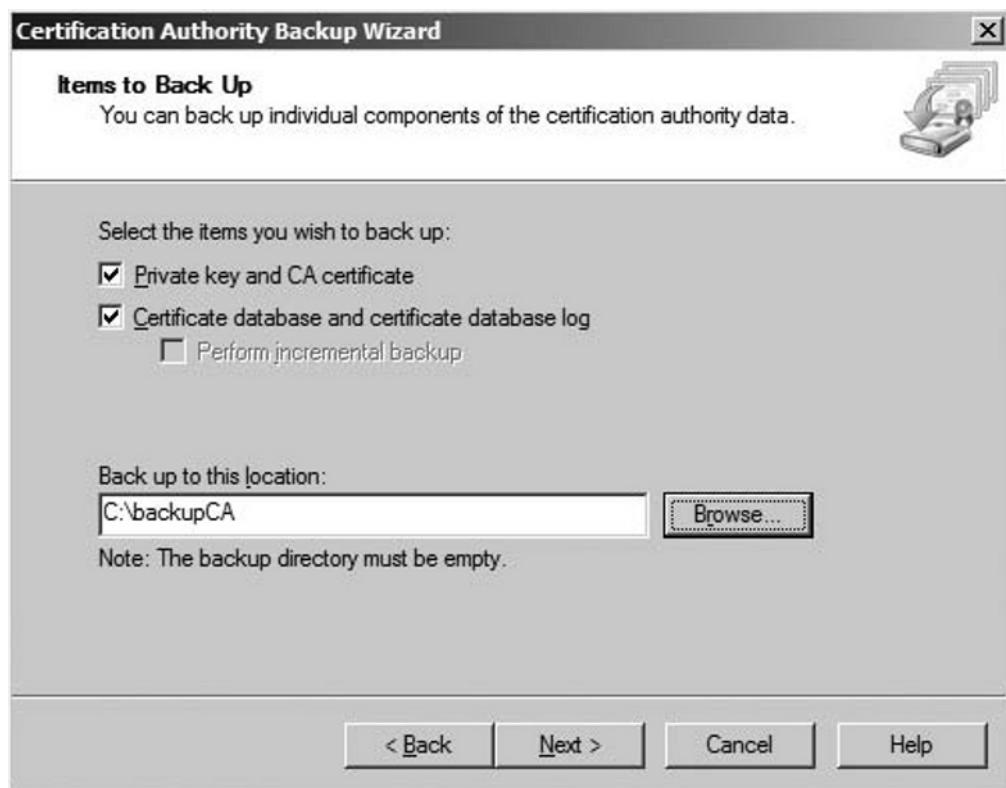
Figure 7.22 Certificate Authority Page



4. On the **Welcome to the Certification Authority Backup Wizard** page, click **Next** to continue.

5. On **Items to Back Up** page, click **Private key and CA certificate** and **Certificate database and certificate database log**. Type in the path of back up location, and then click **Next** (see Figure 7.23).

Figure 7.23 Items to Back Up



6. Type in the backup password twice and click **Next**.
7. On **Completing the Certification Authority Backup Wizard** page, verify it reads as follows: You have successfully completed the **Certification Authority Backup Wizard**, as shown in Figure 7.24.

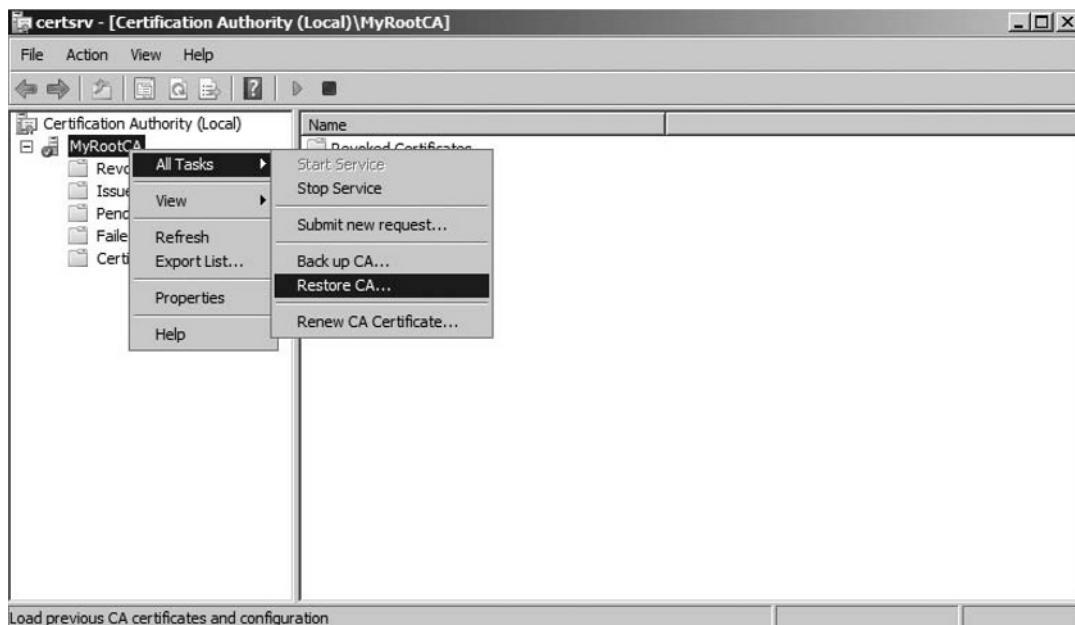
Figure 7.24 Completing the CA Backup Wizard

8. Click **Finish** to close the wizard.

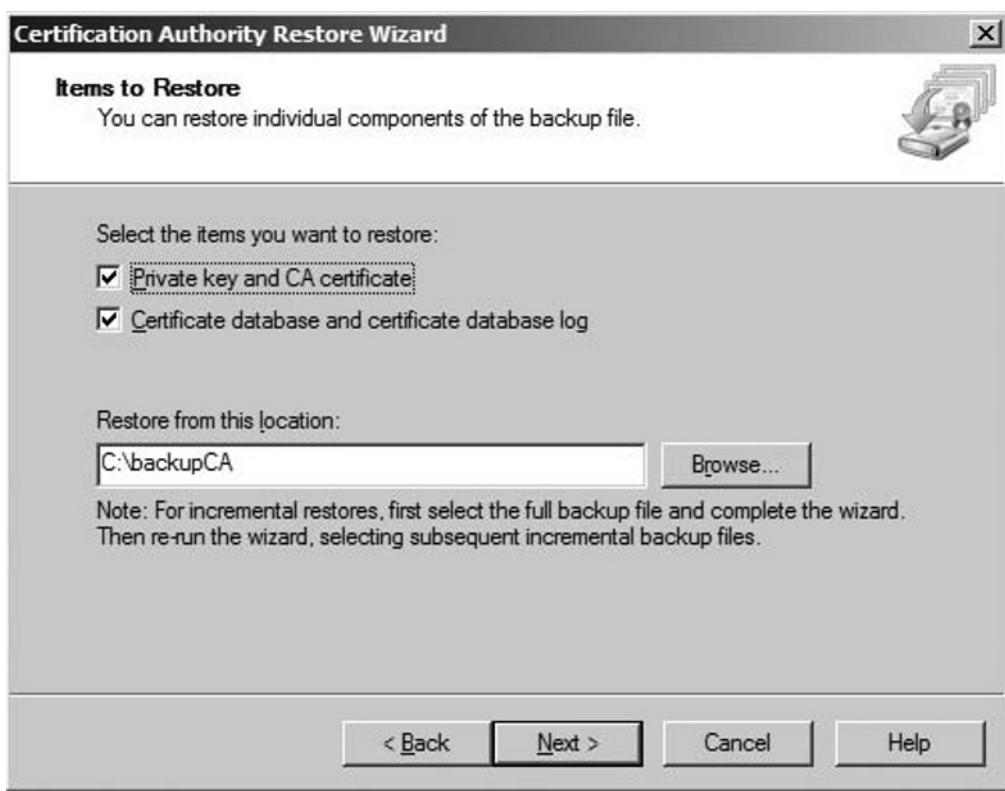
EXERCISE 7.5

RESTORING CERTIFICATE SERVICES

1. On any computer for which you want to take a restore, Log on with administrative privileges.
2. Click **Start**, click **All Programs**, click **Administrative Tools**, and then click **Certification Authority**.
3. Right-click the name of your CA, and choose **All Tasks | Restore CA...** from the pop-up menu, as shown in Figure 7.25.

Figure 7.25 Certificate Authority page

4. Click **OK** to stop Certificate Services from running and start the wizard.
5. On the **Welcome to the Certification Authority Restore Wizard** page, click **Next** to continue.
6. On **Items to Restore** page, click **Private key and CA certificate** and **Certificate database and certificate database log** to restore the backup of **Private key**, **CA certificate**, **Certificate database** and **database log** file (see Figure 7.26). Alternatively, you can choose only few components as per your requirements. Type in the path of back up location, and then click **Next**.

Figure 7.26 Items to Restore

7. On the **Provide Password** page, type in the restore password, and then click **Next**.
8. On **Completing the Certification Authority Restore Wizard** page, verify it reads as You have successfully completed the **Certification Authority Restore Wizard**, as shown in Figure 7.27.

Figure 7.27 Completing the CA Restore Wizard



9. Click **Finish** to complete the wizard.
10. You will now be prompted to restart the certificate services, as shown in Figure 7.28. Click **Yes** to restart the services.

Figure 7.28 Certification Authority Restore Wizard



Assigning Roles

In a small network of one or two servers and just a handful of clients, administration is generally not a difficult task. When the size of the network increases, however, the complexity of administration seems to increase exponentially. Microsoft's recommendations for a large network include dividing administrative tasks among the different administrative personnel. One administrator may be in charge of backups and restores, whereas another administrator may have complete control over a certain domain and so on. The role of each administrator is defined by the tasks that he or she is assigned to, and individual permissions are granted based on those tasks. PKI administration, which can be as daunting as general network administration, can be similarly divided. Microsoft defines five different roles that can be used within a PKI to facilitate administration:

- CA Administrator
- Certificate Manager
- Backup Operator
- Auditor
- Enrollee

At the top of the hierarchy is the CA administrator. The role is defined by the *Manage CA* permission and has the authority to assign other CA roles and to renew the CA's certificate. Underneath the CA administrator is the certificate manager. The certificate manager role is defined by the *Issue and Manage Certificates* permission and has the authority to approve enrollment and revocation requests.

The Backup Operator and the Auditor roles are actually operating system roles, and not CA specific. The Backup Operator has the authority to backup the CA and the Auditor has the authority to configure and view audit logs of the CA. The final role is that of the Enrollees. All authenticated users are placed in this role, and are able to request certificates from the CA.

Enrollments

In order for a PKI client to use a certificate, two basic things must happen. First, a CA has to make the certificate available and second, the client has to request the certificate. Only after these first steps can the CA issue the certificate or deny the request.

Making the certificate available is done through the use of certificate templates and is a topic that we discuss in detail below.

Like Windows Server 2003, Windows Server 2008 PKI also supports autoenrollment for user certificates as well as for computer certificates. The request and issuance of these certificates may proceed without user intervention. Group policies are used in Active Directory to configure autoenrollment. In **Computer Configuration | Windows Settings | Security Settings | Public Key Policies**, there is a group policy entitled **Automatic Certificate Request Settings**. The Property sheet for this policy allows you to choose to either **Enroll certificates automatically** or not. Also, you will need to ensure that **Enroll subject without requiring any user input** option is selected on the **Request Handling** tab of the certificate template Property sheet. Finally, be aware that doing either of the following will cause autoenrollment to fail:

- Setting the **This number of authorized signatures** option on the **Issuance Requirements** tab to higher than one.
- Selecting the **Supply in the request** option on the **Subject Name** tab.



TEST DAY TIP

Remember that autoenrollment is only available for user certificates if the client is Windows XP, Windows Server 2003, or Windows Server 2008.

Revocation

A CA's primary duty is to issue certificates, either to subordinate CAs, or to PKI clients. However, each CA also has the ability to revoke those certificates when necessary. Certificates are revoked when the information contained in the certificate is no longer considered valid or trusted. This can happen when a company changes ISPs (Internet Service Providers), moves to a new physical address or when the contact listed on the certificate has changed. Essentially, a certificate should be revoked whenever there is a change that makes the certificate's information "stale" and no longer reliable from that point forward.

NOTE

Information that has already been encrypted using the public key in a certificate that is later revoked is not necessarily invalid. Maintaining the example of a driver's license, checks that are written and authenticated by a cashier using your driver's license one week are not automatically voided if you lose your license or move states the next.

In addition to the changes in circumstance that can cause a certification revocation, certain owners may have their certificate revoked upon terminating employment. The most important reason to revoke a certificate is if the private key has been compromised in any way. If a key has been compromised, it should be revoked immediately.

EXAM WARNING

Certificate expiration is different from certificate revocation. A certificate is considered revoked if it is terminated prior to the end date of the certificate.

Along with notifying the CA of the need to revoke a certificate, it is equally important to notify all certificate users of the date that the certificate will no longer be valid. After notifying users and the CA, the CA is responsible for changing the status of the certificate and notifying users that it has been revoked.

When a certificate revocation request is sent to a CA, the CA must be able to authenticate the request with the certificate owner. Once the CA has authenticated the request, the certificate is revoked and notification is sent out. CAs are not the only ones who can revoke a certificate. A PKI administrator can revoke a certificate, but without authenticating the request with the certificate owner. This allows for

the revocation of certificates in cases where the owner is no longer accessible or available as in the case of termination.

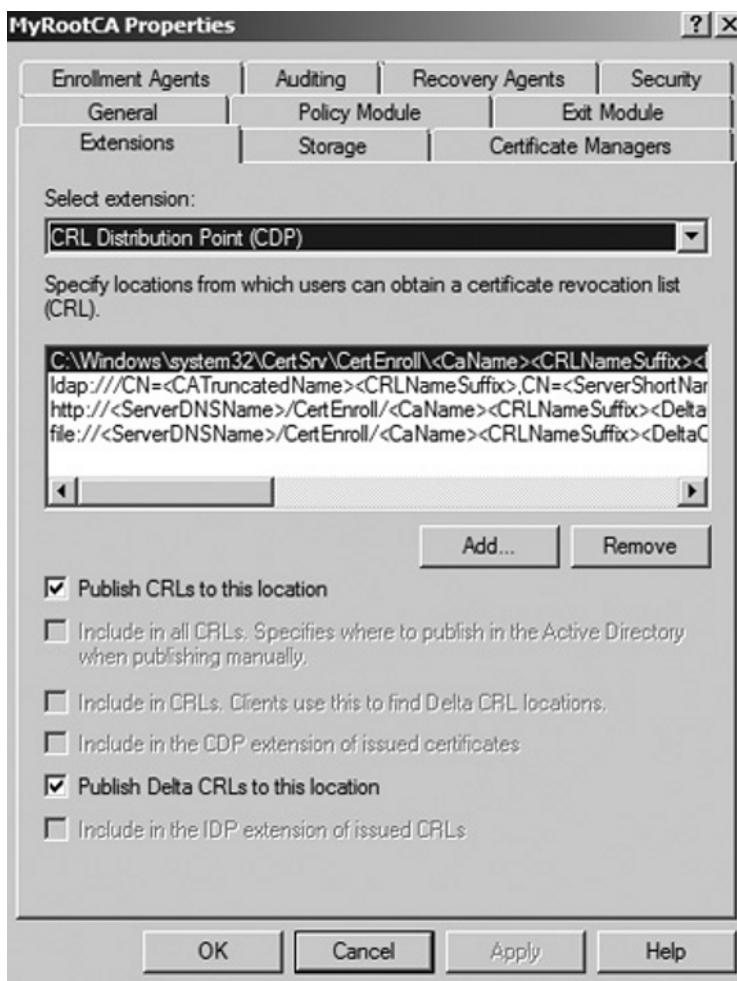
The X.509 standard requires that CA's publish certificate revocation lists (CRLs). In their simplest form, a CRL is a published form listing the revocation status of certification that the CA manages. There are several forms that revocation lists may take, but the two most noteworthy are *simple CRLs* and *delta CRLs*.

A simple CRL is a container that holds a list of revoked certificates with the name of the CA, the time the CRL was published, and when the next CRL will be published. It is a single file that continues to grow over time. The fact that only information about the certificates is included and not the certificate itself helps to manage the size of a simple CRL.

Delta CRLs can handle the issues that simple CRLs cannot- size and distribution. While simple CRLs contain only certain information about a revoked certificate, it can still become a large file. How, then, do you continually distribute a large file to all parties that need to see the CRL? The solution is in Delta CRLs. In an environment leveraging delta CRLs, a base CRL is sent to all end parties to initialize their copies of the CRL. Afterwards, updates known as deltas are sent out on a periodic basis to inform the end parties of any changes.

In practice within Windows Server 2008, the tool that the CA uses for revocation is the *certificate revocation list*, or CRL. The act of revoking a certificate is simple: from the **Certification Authority** console, simply highlight the **Issued Certificates** container, right-click the certificate and choose **All | Revoke Certificate**. The certificate will then be located in the **Revoked Certificates** container.

When a PKI entity verifies a certificate's validity, that entity checks the CRL before giving approval. The question is: how does a client know where to check for the list? The answer is the CDPs, or CRL Distribution Points. CDPs are locations on the network to which a CA publishes the CRL; in the case of an enterprise CA under Windows Server 2008, Active Directory holds the CRL, and for a stand-alone, the CRL is located in the *certsrv\certenroll* directory. Each certificate has a location listed for the CDP, and when the client views the certificate, it then understands where to go for the latest CRL. Figure 7.29 shows the Extensions tab of the CA property sheet, where you can modify the location of the CDP.

Figure 7.29 Extensions Tab of the CA Property Sheet

In order for a CA to publish a CRL, use the **Certificate Authority** console to right-click the **Revoked Certificates** container and choose **All Tasks | Publish**. From there, you can choose to publish either a complete CRL, or a Delta CRL.

TEST DAY TIP

On the day of the test, be clear as to which types of CRLs are consistently made available to users in Windows Server 2008. Since Server 2003, Delta CRLs have been used to publish only the changes made to an original CRL for the purposes of conserving network traffic.

Whether you select a New CRL or a Delta CRL, you are next prompted to enter a publication interval (the most frequent intervals chosen are one week for full CRLs and one day for Delta CRLs). Clients cache the CRL for this period of time, and then check the CDP again when the period expires. If an updated CDP does not exist or cannot be located, the client automatically assumes that all certificates are invalid.

Working with Templates

A *certificate template* defines the policies and rules that a CA uses when a request for a certificate is received. Often when someone refers to building and managing a PKI for their enterprise, they are usually only thinking of the Certificate Authority and the associated infrastructure needed to support the authentication and authorization required to support the function of the CA. While this is certainly important for the proper function of the PKI, it is only half of the picture—the certificates themselves must be carefully planned to support the business goals that are driving the need to install and configure the PKI.

When you consider that certificates are flexible and can be used in scores of different scenarios, the true power of the certificate becomes apparent. While these different uses can all coexist within a single PKI, the types and functions of the certificates can be very different. Certificates that are used to support two-factor authentication on smart cards can be very different than those used to establish SSL connections to web servers, sign IPsec traffic between servers, support 802.1x wireless access through NAP, or even certificates used to sign e-mail communication.

In all of these cases, the CA and the PKI it supports are the same, but it is the certificate itself that is changing. For each of these different uses, it is important for the certificate to contain appropriate data to facilitate in the function that the designer of the PKI has intended and no more. While additional data could be provided in the certificate, the fact that these are intended to mediate security exchanges makes it inappropriate to include any more information than is necessary to complete the certificate's objective. It is the Certificate Template that specifies the data that must be included in a certificate for it to function as well as to ensure that all of the needed data are provided to ensure the certificate's validity.

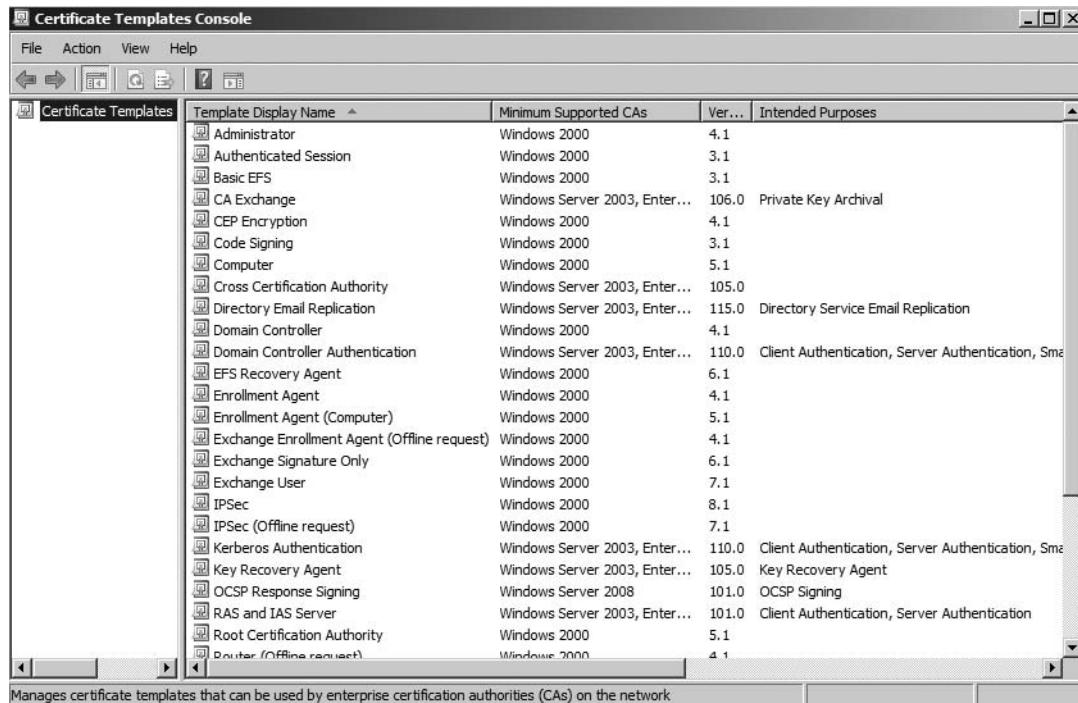
EXAM WARNING

Many different types of certificates can be used together within a single Public Key Infrastructure. It is the Certificate Templates that allow the certificates to differentiate themselves for different purposes ensuring that the appropriate information is stored in the cert.

For an individual certificate, there are a number of properties and settings that go into the certificate template specification. Each of these combine to build the final template that will determine the settings for the resulting Certificate.

There are many built-in templates that can be viewed using the **Certificate Templates** snap-in (see Figure 7.30). The snap-in can be run by right-clicking the **Certificate Templates** container located in the **Certification Authority** console and clicking **Manage**. You can use one of the built-in templates or create your own.

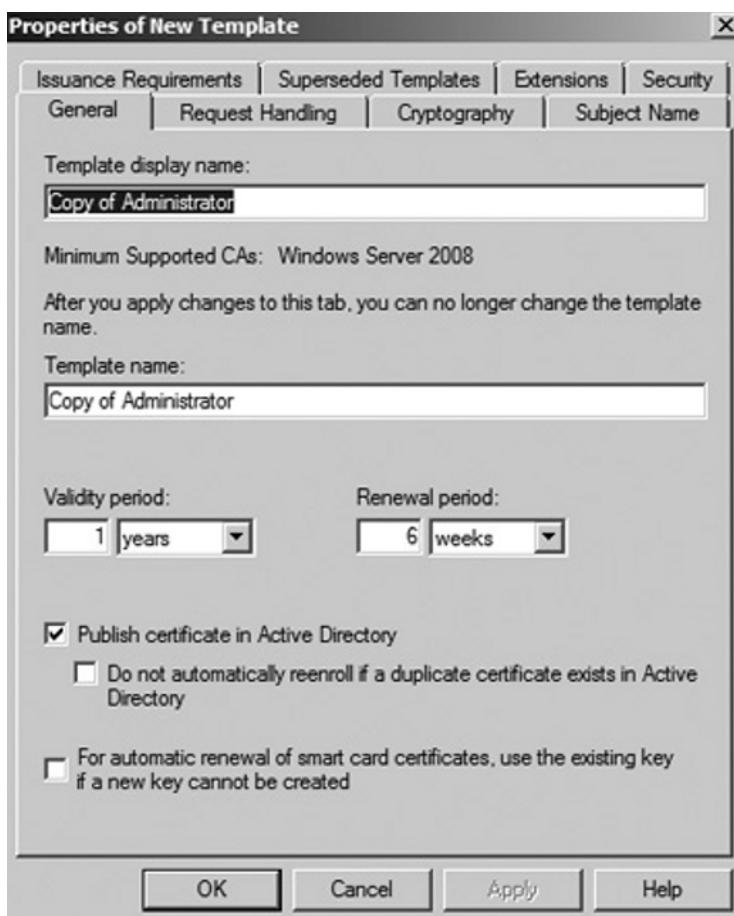
Figure 7.30 Certificate Templates Snap-in



The screenshot shows the 'Certificate Templates Console' window. The title bar reads 'Certificate Templates Console'. The menu bar includes 'File', 'Action', 'View', and 'Help'. Below the menu is a toolbar with icons for back, forward, search, and other functions. The main area is a grid table titled 'Certificate Templates'. The columns are 'Template Display Name', 'Minimum Supported CAs', 'Ver...', and 'Intended Purposes'. The table lists numerous built-in templates, each with a small icon and a brief description. A status bar at the bottom says 'Manages certificate templates that can be used by enterprise certification authorities (CAs) on the network'.

| Template Display Name | Minimum Supported CAs | Ver... | Intended Purposes |
|---|-------------------------------|--------|--|
| Administrator | Windows 2000 | 4.1 | |
| Authenticated Session | Windows 2000 | 3.1 | |
| Basic EFS | Windows 2000 | 3.1 | |
| CA Exchange | Windows Server 2003, Enter... | 106.0 | Private Key Archival |
| CEP Encryption | Windows 2000 | 4.1 | |
| Code Signing | Windows 2000 | 3.1 | |
| Computer | Windows 2000 | 5.1 | |
| Cross Certification Authority | Windows Server 2003, Enter... | 105.0 | |
| Directory Email Replication | Windows Server 2003, Enter... | 115.0 | Directory Service Email Replication |
| Domain Controller | Windows 2000 | 4.1 | |
| Domain Controller Authentication | Windows Server 2003, Enter... | 110.0 | Client Authentication, Server Authentication, Sma... |
| EFS Recovery Agent | Windows 2000 | 6.1 | |
| Enrollment Agent | Windows 2000 | 4.1 | |
| Enrollment Agent (Computer) | Windows 2000 | 5.1 | |
| Exchange Enrollment Agent (Offline request) | Windows 2000 | 4.1 | |
| Exchange Signature Only | Windows 2000 | 6.1 | |
| Exchange User | Windows 2000 | 7.1 | |
| IPSec | Windows 2000 | 8.1 | |
| IPSec (Offline request) | Windows 2000 | 7.1 | |
| Kerberos Authentication | Windows Server 2003, Enter... | 110.0 | Client Authentication, Server Authentication, Sma... |
| Key Recovery Agent | Windows Server 2003, Enter... | 105.0 | Key Recovery Agent |
| OCSP Response Signing | Windows Server 2008 | 101.0 | OCSP Signing |
| RAS and IAS Server | Windows Server 2003, Enter... | 101.0 | Client Authentication, Server Authentication |
| Root Certification Authority | Windows 2000 | 5.1 | |
| Router (Offline request) | Windows 2000 | 4.1 | |

When creating your own template, you have multiple options that will guide the CA in how to handle incoming requests. The first step in the creation process is to duplicate an existing template. You do this by using the **Certificate Templates** snap-in, then right-clicking the template you wish to copy and selecting *Duplicate Template*. On the **General** tab that appears by default (seen in Figure 7.31), there are time-sensitive options such as validity period and renewal period. Note the default validity period of one year, and the default renewal period of six weeks. There are also general options such as the template display name and a checkbox for publishing the certificate in Active Directory.

Figure 7.31 General Tab of the New Template Property Sheet

General Properties

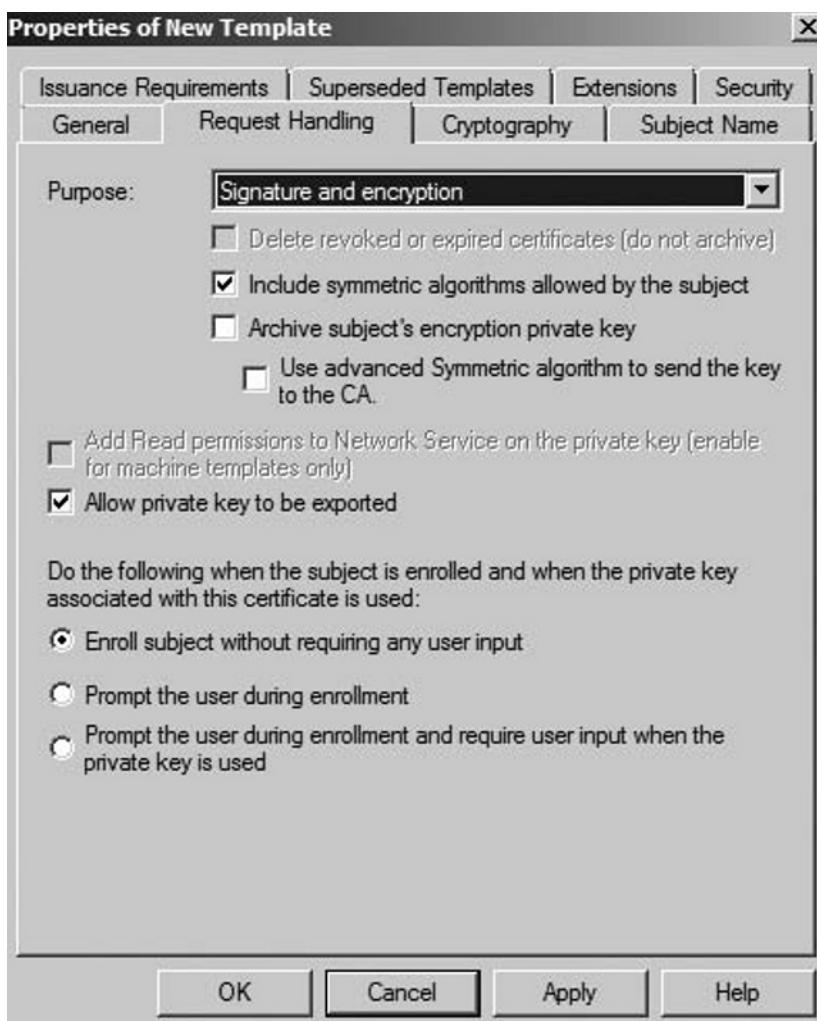
Now we'll describe the following settings under the General tab of the new certificate template:

- **Template Display Name** It is important that the certificate that you are creating has a descriptive name accurately describes the function of the certificate. This name cannot be changed once it is assigned, but you can always recreate the certificate from another template later.
- **Validity Period** This is the period for which the derived certificates are valid. This time should be long enough so as not to create a burden on the end user, but not so long as to create a security problem.

- **Renewal Period** This is the period in which the certificate is notified of its expiration and that it will attempt to renew if this is an option for the certificate.
- **Publish in Active Directory** Some certificates can be stored in the active directory tied to security principals there. This generally applies to User certificates that are not tied to specific hardware.

The **Request Handling** tab, shown in Figure 7.32, has options to enroll without user interaction.

Figure 7.32 Request Handling Tab of the New Template Property Sheet

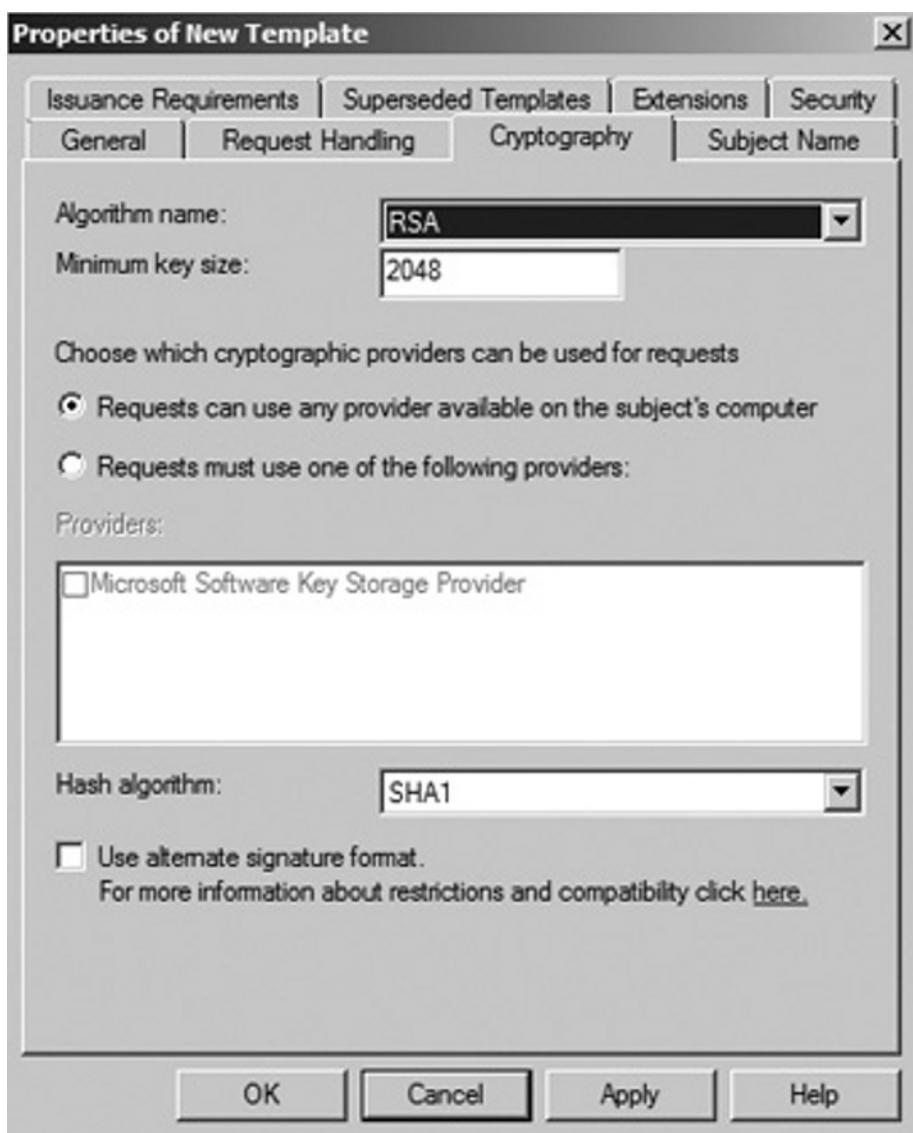


Request Handling

The Request Handling tab includes the following settings:

- **Purpose** It is important to consider the activities for which this new certificate will be responsible. Some keys can be used just to validate identity while others can also provide signing for encryption.
 - The private key can also be archived or shared with the CA so that it may be recovered in the event of loss. Otherwise, the certificate must be recreated.
- **Enrollment Actions** Different notification actions can be specified when the private key for this certificate is used. This can range from transparent usage of the key to full notification prompting the certificate owner for permission.

The **Cryptography** tab seen in Figure 7.33, gives you the choice of algorithms that can be used.

Figure 7.33 Cryptography Tab

Cryptography

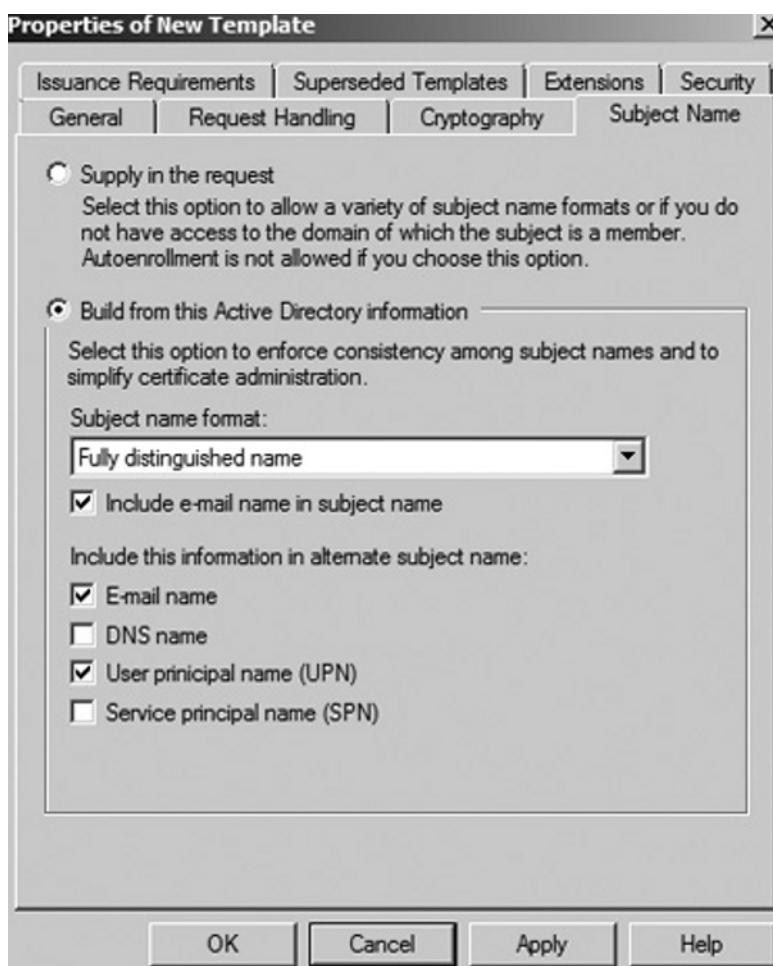
The Cryptography tab includes the following settings:

- **Algorithm Name** There are a number of cryptographic Algorithms that can be used to provide encryption for the keys. Valid methods under server 2008 are RSA, ECDH_P256, ECDH_P384, ECDH_P521.

- Note: If the Purpose is changed to Signature, additional algorithms become available: ECDSA_P256, ECDSA_P384, ECDSA_P521.
- **Hash Algorithm** To provide one-way hashes for key exchanges, a number of algorithms are available. These include: MD2, MD4, MD5, SHA1, SHA256, SHA384, SHA512.

The **Subject Name** tab seen in Figure 7.34, gives you the choice of obtaining subject name information from Active Directory or from the certificate request itself. In the latter case, autoenrollment (which we'll discuss later in the chapter) is not available.

Figure 7.34 Subject Name Tab of the New Template Property Sheet



Subject Name

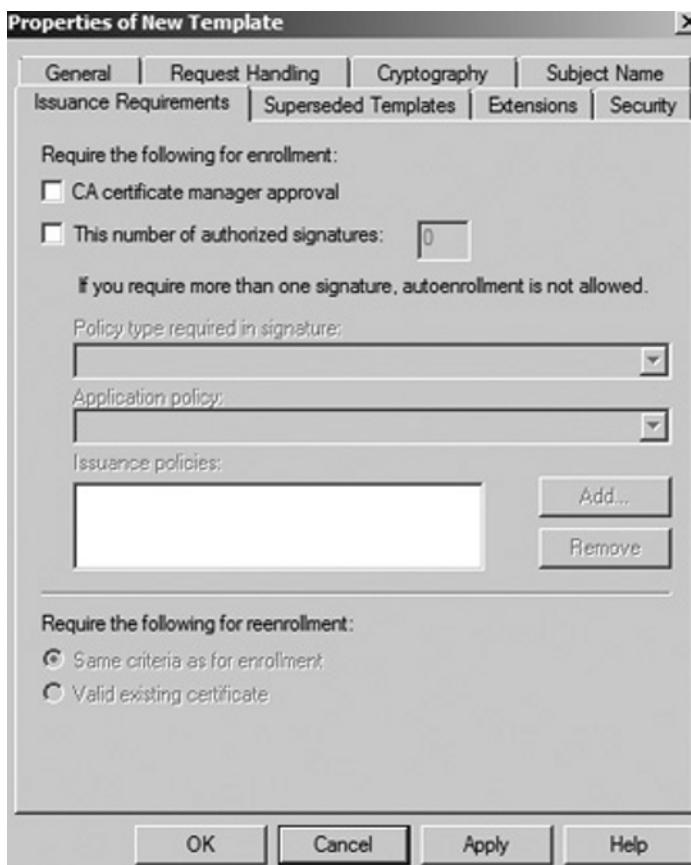
The Subject Name tab includes the following settings:

- **Supply in the Request** Under this option, the CA will expect to get additional subject information in the certificate request. As noted, this will not permit autoenrollment, requiring intervention to issue the certificate.
- **Build from this AD Information** Under this option, the Active Directory will be queried and the certificate will be built based on the AD files you specify.

Usually the default of the Distinguished Name is adequate for most purposes, but the common name will sometime be preferable.

The **Issuance Requirements** tab seen in Figure 7.35 allows you to suspend automatic certificate issuance by selecting the CA certificate manager approval checkbox.

Figure 7.35 Issuance Requirements Tab of the New Template Property Sheet



Issuance Requirements

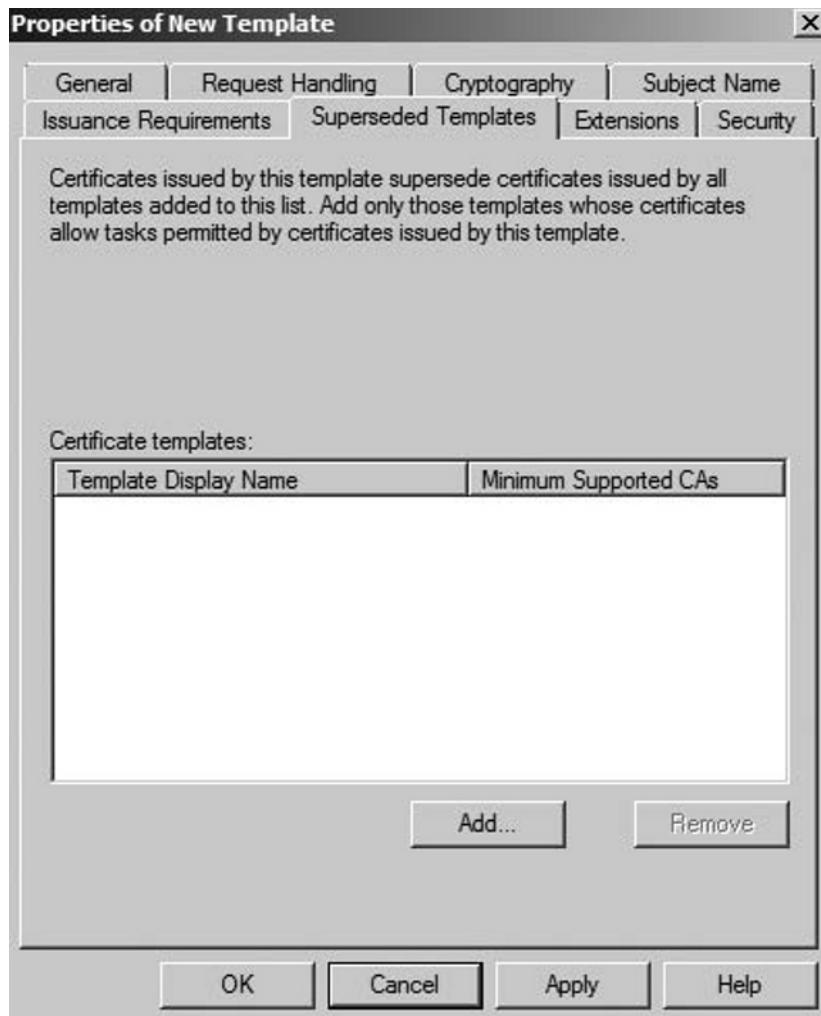
These settings can be used to manage the approval requirements in order for a certificate to be issued. These settings allow for a workflow or approval chain to be applied to the certificate type.

- **CA Certificate Manager Approval** Using this setting will require that the CA Manager assigned in the CA approve of the certificate before it is released to the end-user of the certificate.
- **Number of Authorized Signatures** Under these settings, additional approvals steps may be required to release the certificate. In these scenarios, two or more approval authorities will have to consent before the certificate is generated.
- **Require the Following for Reenrollment** These settings specify the approval and prerequisites that are in place for renewal of the certificate. This gives the network administrator to allow subjects with valid certificates to renew without having to go through the approval chain.

The **Superseded Templates** tab, as shown in Figure 7.36, is used to define which certificates are superseded by the current template. Usually, this tab is used to configure a template that serves several functions, e.g. IPsec and EFS. In this case, a template used *only* for IPsec or a template used *only* for EFS would be placed on the superseded templates list. This section allows the network administrator to specify other templates that are superseded by the new template type. This allows control of both versioning and wholesale template replacement.

As templates evolve, it may be useful to replace templates that are already deployed in the wild with a new template.

Figure 7.36 Superseded Templates Tab of the New Template Property Sheet



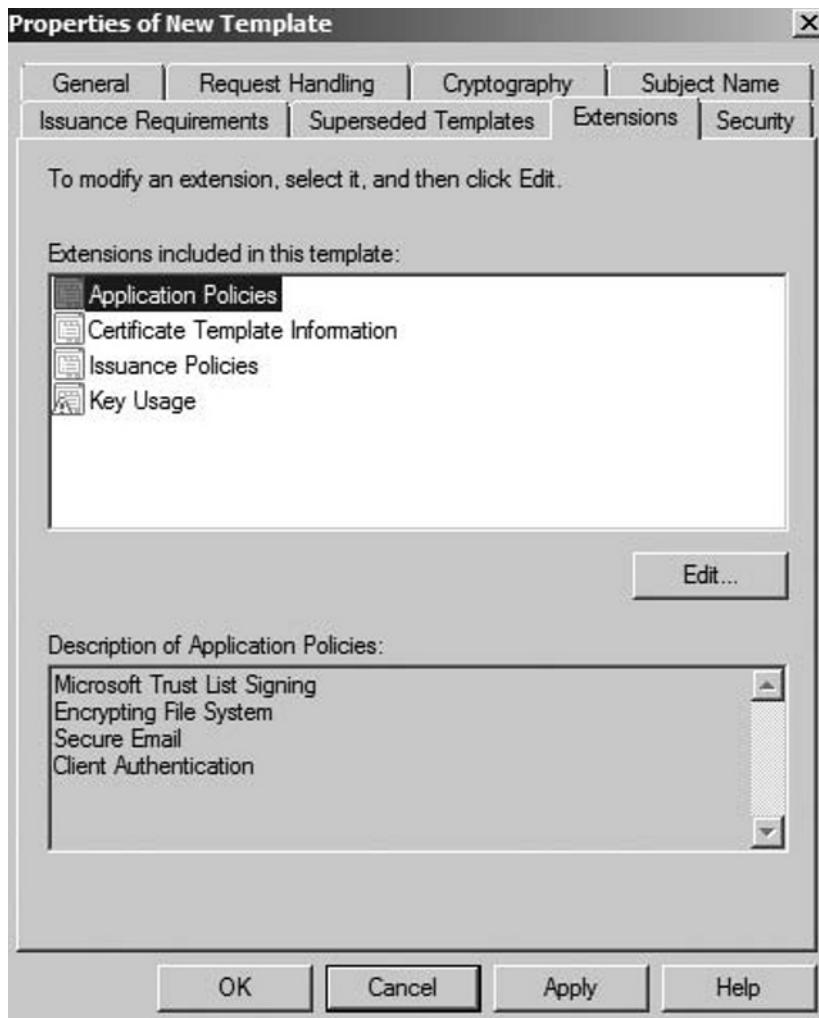
In addition to the standard usage patterns that are inherited from the parent certificate, it is sometimes important to specify new circumstances and roles that a certificate will fill. In this case, additional extensions to the certificate will be applied to provide this new functionality.

Under these settings, a new ability such as code signing can be applied to all derivative certificates to allow these new subjects the ability to complete multiple tasks.

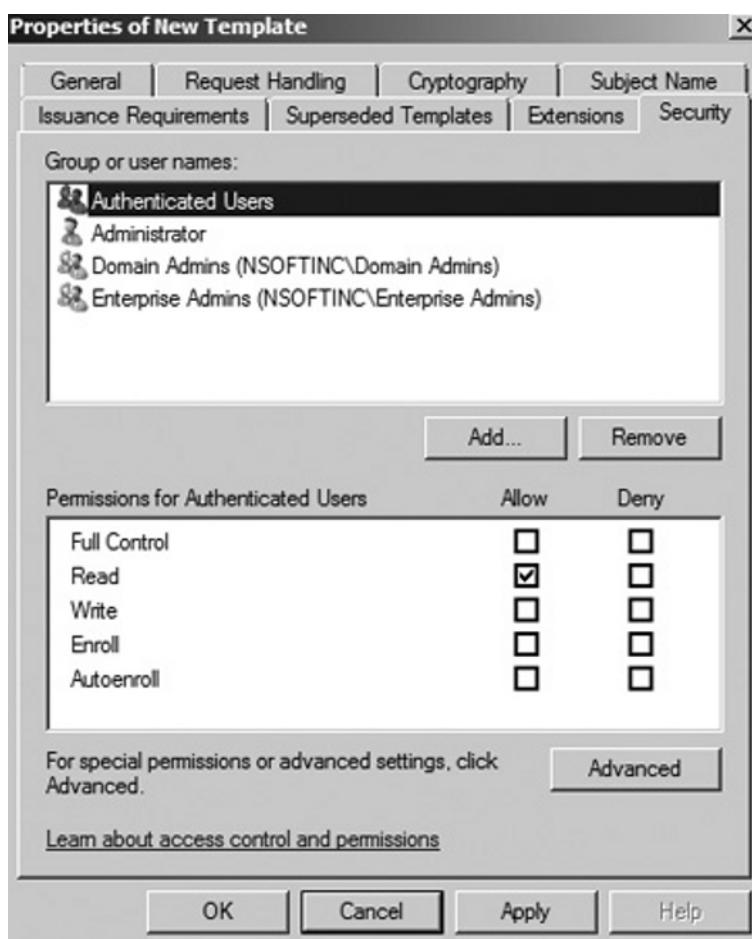
The **Extensions** tab as seen in Figure 7.37 can be used to add such things as the Application Policies extension, which defines the purposes for which a generated

certificate can be used. The Issuance Policies extension is also worth mentioning, because it defines when a certificate may be issued.

Figure 7.37 Extensions Tab of the New Template Property Sheet



The **Security** tab is similar to the **Security** tab that we saw in Figure 7.38, except that this tab is used to control who may edit the template and who may request certificates using the template. Figure 7.38 shows the default permission level for the **Authenticated Users** group. In order for a user to request a certificate, however, the user must have at least the **Enroll** permission assigned to them for manual requests, and the **Autoenroll** permission for automatic requests.

Figure 7.38 Security Tab of the New Template Property Sheet

Security

The security settings control the actions that different types of users are able to perform on a certificate template.

- **Enroll** These subjects are able to request that a certificate be created from this template and assigned to them. This enrollment process will abide by the constraints listed under the Issuance Requirements tab.
- **Autoenroll** These subjects are able to make a request to the CA and will be automatically issued the certificate if the subject meets the Issuance Requirements. In this case, the certificate will be applied without administrator intervention or assistance.

After you have configured a particular template, it still cannot be used by the CA to issue certificates until it is made *available*. To enable a template, you use the **Certification Authority** console and right-click the **Certificate Templates** container. Selecting **New | Certificate Template to Issue** completes the process.

Types of Templates

There are a number of different templates that are included with Windows Server 2008 that provide basic signing and encryption services in the Enterprise Windows PKI role. In addition to these pre-built templates, the network administrator also has the option to build custom templates to address needs that might not be covered by the standard templates or to provide interoperation with other systems.

The Subject Field of the Certificate templates determines the scope of action and the types of objects to which the resulting certificates can be bound.

User Certificate Types

User Certificate Templates are intended to be bound to a single user to provide identity and/or encryption services for that single entity.

- **Administrator** This certificate template provides signature and encryption services for administrator accounts providing account identification and trust list (CTL) management within the domain. Certificates based on the Administrator Template are stored in the Active Directory.
- **Authenticated Session** This certificate template allows users to authenticate to a web server to provide user credentials for site logon. This is often deployed for remote users as a way to validate identity without storing formation insecurely in a cookie while avoiding the need for a user to log on to the site each time.
- **Basic EFS** Certificates derived from this template are stored in Active Directory with the associated user account and are used to encrypt data using the Encrypting File System (EFS).
- **Code Signing** These certificate templates allow developers to create certificates that can be used to sign application code. This provides a check on the origin of software so that code management systems and end-users can be sure that the origin of the software is trusted.
- **EFS Recovery Agent** Certificates of this type allow files that have been encrypted with the EFS to be decrypted so that the files can be used again.

EFS Recovery Agent certificates should be a part of any disaster recovery plan when designing an EFS implementation.

- **Enrollment Agent** Certificates derived from this template are used to request and issue other certificates from the enterprise CA on behalf of another entity. For example, the web enrollment application uses these certificates to manage the certificate requests with the CA.
- **Exchange Enrollment Agent** These certificates are used to manage enrollment services form within exchange to provide certificates to other entities within the exchange infrastructure.
- **Exchange Signature** Certificates derived from the Exchange Signature template are user certificates used to sign e-mail messages sent from within the Exchange system.
- **Exchange User** Certificates based on the Exchange User template are user certificates that are stored in the Active Directory used to encrypt e-mail messages sent from within the Exchange system.
- **Smartcard Logon** These certificates allow the holder of the smart card to authenticate to the active directory and provides identity and encryption abilities. This is usually deployed as a part of a two-factor security schema using smart cards as the physical token.
- **Smartcard User** Unlike the Smartcard Logon certificate template, these types of certificates are stored in the Active Directory and limit the scope of identity and encryption to e-mail systems.
- **Trust List Signing** These certificates allow the signing of a trust list to help manage certificate security and to provide affirmative identity to the signer.
- **User** This template is used to create general User Certificates—the kind that are usually thought of when talking about user certificates. These are stored in the Active Directory and are responsible for user activities in the AD such as authentication, EFS encryption, and interaction with Exchange.
- **User Signature Only** These certificates allow users to sign data and provide identification of the origin of the signed data.

Computer Certificate Types

Computer Certificate Templates are intended to be bound to a single computer entity to provide identity and/or encryption services for that computer. These are

often the cornerstone of workstation authentication systems like NAP and 802.1x which might require computer certificates for EAP authentication.

- **CA Exchange** These certificates are bound to Certificate Authorities to mediate key exchange between CAs allowing for PK sharing and archival.
- **CEP Encryption** Certificates of this type are bound to servers that are able to respond to key requests through the Simple Certificate Enrollment Protocol (SCEP).
- **Computer** This template is used to generate standard Computer certificates that allow a physical machine to assert its identity on the network. These certificates are extensively used in EAP authentication in identifying endpoints in secured communication tunnels.
- **Domain Controller Authentication** Certificates of this type are used to authenticate users and computers in the active directory. This allows a Domain Controller to access the directory itself and provide authentication services to other entities.
- **Enrollment Agent (Computer)** These certificates allow a computer to act as an enrollment agent against the PKI so that they can offer computer certificates to physical machines.
- **IPsec** Certificates based on this template allow a computer to participate in IPsec communications. These computers are able to assert their identity as well as encrypt traffic on the network. This is used in IPsec VPN tunnels as well as in Domain and Server Isolation strategies.
- **Kerberos Authentication** These certificates are used by local computers to authenticate with the Active Directory using the Kerberos v5 protocol.
- **OCSP Response Signing** This is a unique certificate type to Windows Server 2008 allowing a workstation to act as an Online Responder in the validation of certificate request queries.
- **RAS and IAS Server** These certificates are used to identify and provide encryption for Routing and Remote Access Server (RRAS) as well as Internet Authorization Servers (IAS) to identify themselves in VPN and RADIUS communications with RADIUS Clients.
- **Router** This is also a new role to Windows Server 2008 providing services to provide credentials to routers making requests through SCEP to a CA.

- **Web Server** These certificates are commonly used by servers acting as web servers to provide end-point identification and traffic encryption to their customers. These kinds of certificates are used to provide Secure Socket Layer (SSL) encryption enabling clients to connect to the web server using the HTTPS protocol.
- **Workstation Authentication** Like general computer certificates, the workstation certificate allows computers that are domain members the ability to assert their identity on the network and encrypt traffic that they send across the network.

Other Certificate Types

There are a number of other certificate types that are not directly tied to either user or computer entities. These are usually infrastructure-based certificate types that are used to manage the domain or the Certificate Authorities themselves.

- **Cross-Certification Authority** These certificates are used within the Certificate Authority Infrastructure to cross-certify CAs to validate the hierarchy that makes up the PKI.
- **Directory E-mail Replication** Certificates that are derived from this type are used within the larger Exchange infrastructure to allow for the replication of e-mail across the directory service.
- **Domain Controller** This kind of certificate is only held by the Domain Controllers in the domain. These differentiate from the Domain Controller Authentication certificates as they identify the individual DC rather than facilitate authorization of inbound authentication requests.
- **Root CA** These certificates are only issued to Root Certificate Authorities to assert its identity in the Public Key Infrastructure.
- **Subordinate CA** This certificate type is used to assert the identity of Subordinate Certificate Authorities in the PKI. This type of certificate can only be issued by a computer holding the Root CA certificate or another Subordinate CA that is the direct parent of the one to which the new certificate is being issued.

Custom Certificate Templates

In some circumstances, it might be necessary to create a custom certification type that can be used to support a specific business need. If you are using a version of

Windows Server 2008 that is not either the WEB or Standard edition, you can create your own templates.

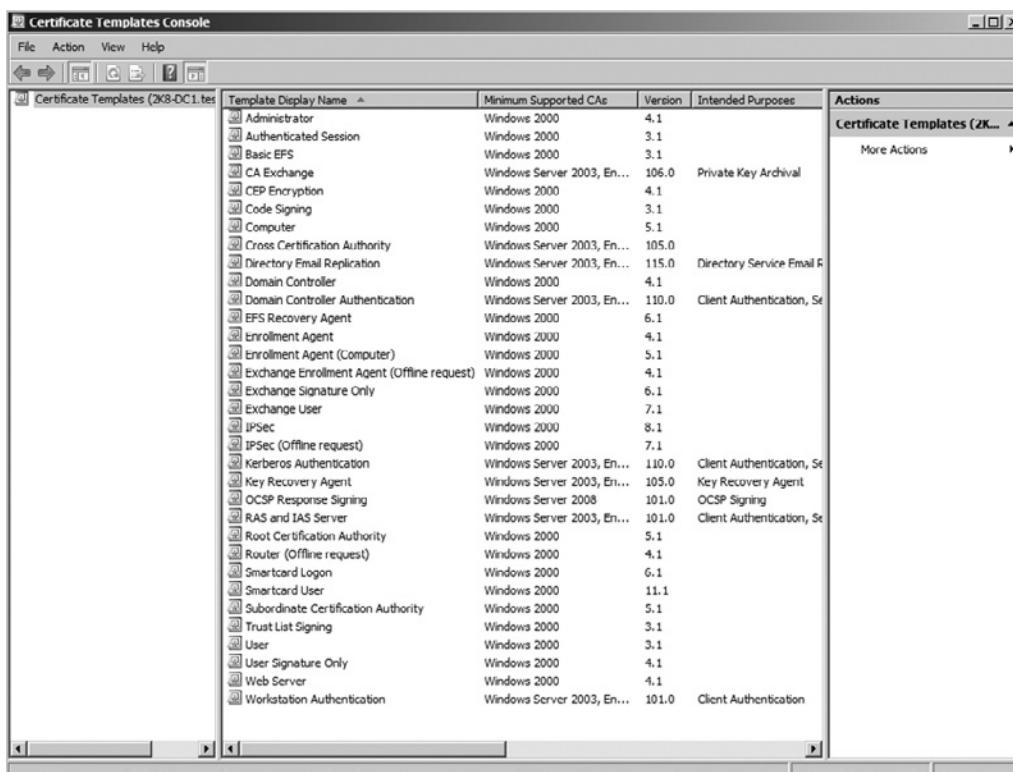
EXERCISE 7.6

CREATING A CUSTOM TEMPLATE

In this exercise, we will create a new User Template based on the existing default user template. This new template will be valid for 10 years rather than the default 1-year expiration date.

1. Log in to your domain with an account that is a member of the Domain Admins group.
2. Navigate to **Start | Administrative Tools | Certificate Authority**.
3. Right-click the **Certificate Templates** folder on the left pane. Choose **Manage** to open the Certificate Templates Console (see Figure 7.39).

Figure 7.39 Creating a Custom Template

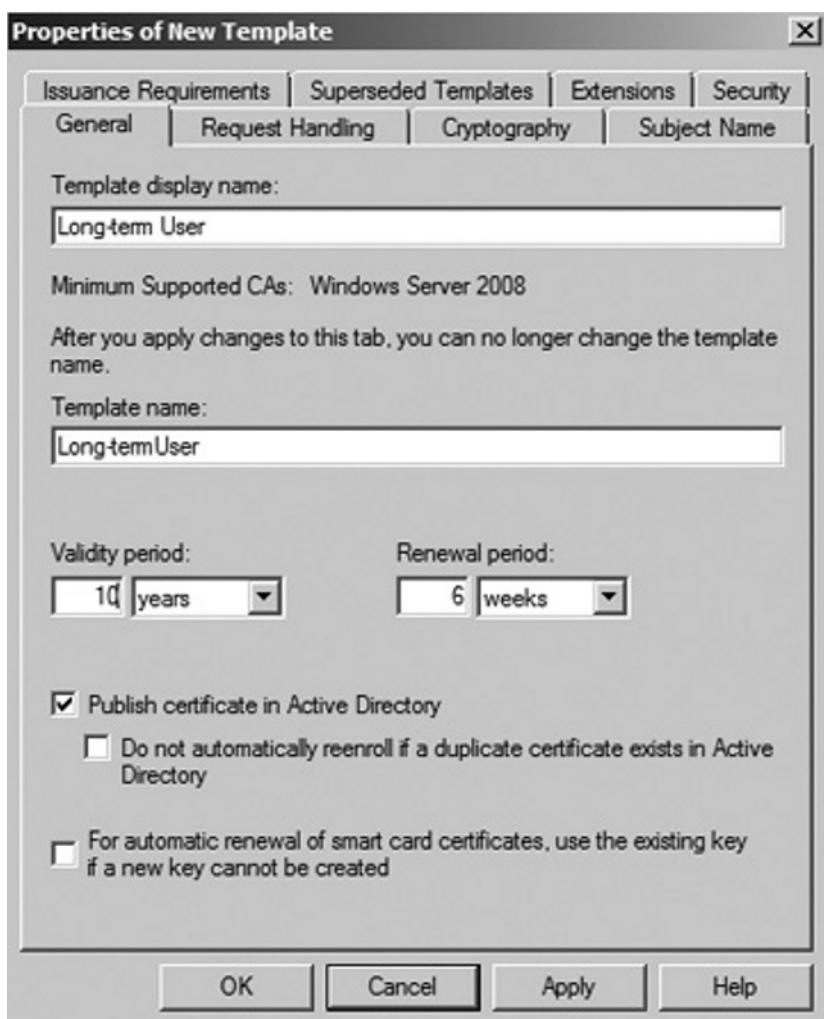


4. Right-click the **User Template**. Choose **Duplicate Template**.
5. On the Duplicate Template page, choose **Server 2008** versioning as all of our CAs are running Server 2008 (see Figure 7.40). Click **OK**.

Figure 7.40 Creating a Custom Template



6. In the **Template display name**, enter **Long-term User**.
7. Change the **Validity Period** to 10 Years (see Figure 7.41).

Figure 7.41 Creating a Custom Template

8. Click OK.

The new Long-term User certificate template has now been created on this CA and is ready to be used to create new derivative certificates.

Securing Permissions

With the wide set of configuration options that are available when creating a new Certificate Template, it might come as a surprise that the permissions model is relatively simple. All of the more complicated security controlling the approval

process and revocation is already built into the Certificate Template itself, so there is little left to control through the more traditional Access Control Entries on the template's Access Control List.

- **Full Control** Users with this permission have access to do anything with the Certificate Template. Users with this right should be confined to the Domain Administrators and CA Managers who will be maintaining the CA and the associated Templates.
- **Read** These users will be able to read the template and view its contents. It is important for users to be able to Read the template if they are to apply it and continue to use the associated certificates issued from the template.
- **Write** Users who are able to modify and manage the template will need to have write permissions on the template. Again, this should be confined to Domain Administrators and CA Managers who will be responsible for maintaining the Templates.
- **Enroll** Users who will request certificates of this type or who already have these certs will need to have Enroll privileges.
- **AutoEnroll** Subjects that will request new certificates through the autoenrollment process will need to have autoenrollment privileges in addition to the enroll and read permissions.



NOTE

In order to keep the Certificate Authority communicating with the Active Directory, it is important that the Cert Publishers group be protected. Make sure that this group is not inadvertently destroyed or changed.

Versioning

Certificates are all tagged with version information allowing them to evolve over time. Without this feature, when a Certificate Template would get updated, all of the certificates based on the old template would have to be revoked forcing the end-users to apply for new certificates again. This is disruptive to business and introduces a large amount of risk to business continuity as the certificates are brought into compliance again.

With versioning, a new version of the Certificate Template can be issued into the production environment. Then using the autoenrollment process, these certificates can be superseded bring all of the certificate holding subjects into compliance quickly and with a minimum of both disruption to the business and administrative intervention.

EXAM WARNING

In an environment that has been upgraded from a previous version of Windows Server into the Server 2008 platform, an update to the certificate templates may be required to bring the templates into compliance. This should be done before the domain is upgraded to ensure continuity with the active directory.

Key Recovery Agent

Sometimes it is necessary to recover a key from storage. One of the problems that often arise regarding PKI is the fear that documents will become lost forever—irrecoverable because someone loses or forget their private key. Let's say that employees use Smart Cards to hold their private keys. If a user were to leave his smart card in his wallet which was left in the pants that he accidentally threw into the washing machine, then that user might be without his private key and therefore incapable of accessing any documents or e-mails that used his existing private key.

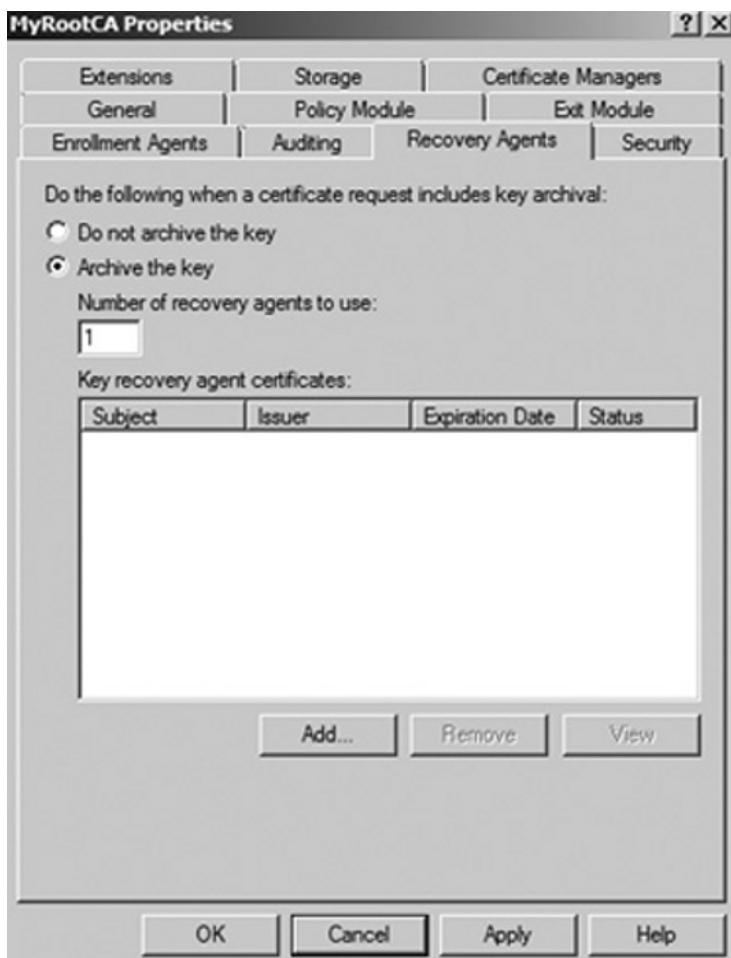
Many corporate environments implement a key recovery server solely for the purpose of backing up and recovering keys. Within an organization, there is at least one *key recovery agent*. A key recovery agent is an employee who has the authority to retrieve a user's private key. Some key recover servers require that two key recovery agents retrieve private user keys together for added security. Some key recovery servers also have the ability to function as a key escrow server, thereby adding the ability to split the keys onto two separate recovery servers, further increasing security.

Luckily, Windows Server 2008 provides a locksmith of sorts (called a Registration Authority, or RA) that earlier versions of Windows did not have. A key recovery solution, however, is not easy to implement and requires several steps. The basic method follows:

1. Create an account to be used for key recovery.
2. Create a new template to issue to that account.
3. Request a key recovery certificate from the CA.

4. Have the CA issue the certificate.
5. Configure the CA to archive certificates by using the **Recovery Agents** tab of the CA property sheet (shown in Figure 7.42).
6. Create an archive template for the CA.

Figure 7.42 Recovery Agents Tab of the CA Property Sheet



Each of these steps requires many substeps, but can be well worth the time and effort. It is worth noting again that key recovery is not possible on a stand-alone CA, because a stand-alone cannot use templates. It is also worth noting that only encryption keys can be recovered—private keys used for digital signatures cannot.

Summary of Exam Objectives

The purpose of a PKI is to facilitate the sharing of sensitive information such as authentication traffic across an insecure network. This is done with public and private key cryptography. In public key cryptography, keys are generated in pairs so that every public key is matched to a private key and vice versa. If data is encrypted with a particular public key, then only the corresponding private key can decrypt it. A digital signature means that an already encrypted piece of data is further encrypted by someone's private key. When the recipient wants to decrypt the data, he or she must first "unlock" the digital signature by using the signer's public key, remembering that only the *signer's* public key will work. This might seem secure, but because anyone at all can sign the data, how does the recipient know for certain the identity of the person who actually signed it?

The answer is that digital signatures need to be issued by an authoritative entity, one whom everyone trusts. This entity is known as a certification authority. An administrator can use Windows Server 2008, a third-party company such as VeriSign, or a combination of the two to create a structure of CAs. Certification authorities, as the name implies, issue certificates. In a nutshell, certificates are digitally signed public keys. Certificates work something like this: party A wants to send a private message to party B, and wants to use party B's public key to do it. Party A realizes that if B's public key is used to encrypt the message, then only B's private key can be used to decrypt it and since B and no one else has B's private key, everything works out well. However, A needs to be sure that he's really using B's public key and not an imposter's, so instead of just asking B for B's public key, he asks B for a certificate. B has previously asked the CA for a certificate for just such an occasion (B will present the certificate to anyone who wants to verify B's identity). The CA has independently verified B's identity, and has then taken B's public key and signed it with its own private key, creating a certificate. A trusts the CA, and is comfortable using the CA's well-known public key. When A uses the CA's public key to unlock the digital signature, he can be sure that the public key inside really belongs to B, and he can take that public key and encrypt the message.

The "I" in PKI refers to the infrastructure, which is a system of public key cryptography, certificates, and certification authorities. CAs are usually set up in a hierarchy, with one system acting as a root and all the others as subordinates at one or more levels deep. By analyzing the certificate requirements for your company, you can design your CA structure to fit your needs. Most organizations use a three-tier model, with a root CA at the top, an intermediate level of subordinates who control CA policy, and a bottom level of subordinates who actually issue certificates to users,

computers, and applications. In addition to choosing root and subordinate structure for the CA hierarchy, each CA during installation needs to be designated as either an enterprise or a stand-alone. Each of these choices has distinct advantages and disadvantages. Most CA configuration after installation is done through the Certification Authority snap-in. In addition to issuing certificates, CAs are also responsible for revoking them when necessary. Revoked certificates are published to a CRL that clients can download before accepting a certificate as valid.

Enterprise CAs use templates to know what to do when a certificate request is received and how to issue a certificate if approved. There are several built-in templates included in Server 2008, or you can configure new ones. Once a CA is ready to issue certificates, clients need to request them. Autoenrollment, Web enrollment, or manual enrollment through the Certificates snap-in are the three ways by which a client can request a certificate. Autoenrollment is available for computer certificates, and in Windows Server 2008, for user certificates as well.

Exam Objectives Fast Track

Planning a Windows Server 2008 Certificate-Based PKI

- A PKI combines public key cryptography with digital certificates to create a secure environment where network traffic such as authentication packets can travel safely.
- Public keys and private keys always come in pairs. If the public key is used to encrypt data, only the matching private key can decrypt it.
- When public key-encrypted data is encrypted again by a private key, that private key encryption is called a digital signature.
- Digital signatures provided by ordinary users aren't very trustworthy, so a trusted authority is needed to provide them. The authority (which can be Windows-based) issues certificates, which are basically digitally signed containers for public keys and other information.
- Certificates are used to safely exchange public keys, and provide the basis for applications such as IPsec, EFS, and smart card authentication.

Implementing Certification Authorities

- Certificate needs are based on which applications and communications an organization uses and how secure they need to be. Based on these needs, CAs are created by installing certificate services and are managed using the Certification Authority snap-in.
- A CA hierarchy is structured with a root and one or more level of subordinates—three levels are common. The bottom level of subordinates issues certificates. The intermediate level controls policies.
- Enterprise CAs require and use Active Directory to issue certificates, often automatically. Stand-alone CAs can be more secure, and need an administrator to manually issue or deny certificate requests.
- CAs need to be backed up consistently and protected against attacks. Keys can be archived and later retrieved if they are lost. This is a new feature for Windows Server 2008.
- CAs can revoke as well as issue certificates. Once a certificate is revoked, it needs to be published to a CRL distribution point. Clients check the CRL periodically before they can trust a certificate.

Planning Enrollment and Distribution of Certificates

- Templates control how a CA acts when handed a request, and how to issue certificates. There are quite a few built-in templates, or you can create your own using the Certificate Template snap-in. Templates must be enabled before a CA can use them.
- Certificates can be requested with the Certificates snap-in or by using Internet Explorer and pointing to <http://servername/certsrv> on the CA.
- Machine and user certificates can be requested with no user intervention requirement by using autoenrollment. Autoenrollment for user certificates is new to Windows Server 2008.
- Role-based administration is recommended for larger organizations. Different users can be assigned permissions relative to their positions, such as certificate manager.

Exam Objectives

Frequently Asked Questions

Q: In what format do CAs issue certificates?

A: Microsoft certificate services use the standard X.509 specifications for issued certificates and the Public Key Cryptography Standard (PKCS) #10 standard for certificate requests. The PKCS #7 certificate renewal standard is also supported. Windows Server 2003 also supports other formats, such as PKCS #12, DER encoded binary X.509, and Base64 Encoded X.509, for exporting certificates to computers running non-Windows operating systems.

Q: If certificates are so important in a PKI, why don't I see more of them?

A: Many portions of a Windows PKI are hidden to the end user. Thanks to features such as autoenrollment, some PKI transactions can be completely done by the operating system. Most of the work in implementing a PKI comes in the planning and design phase. Operations such as encrypting data via EFS use certificates, but the user does not "see" or manually handle the certificates.

Q: I've heard that I can't take my laptop overseas because it uses EFS. Is this true?

A: Maybe. The backbone of any PKI-enabled application such as EFS is encryption. Although the U.S. government now permits the exporting of "high encryption" standards, some countries still do not allow their import. The Windows Server 2008 PKI can use high encryption, and so the actual answer depends on the country in question. For information on the cryptographic import and export policies of a number of countries, see <http://www.rsasecurity.com/rsalabs/faq/6-5-1.html>.

Q: Can I create my own personal digital signature and use it instead of a CA?

A: Not if you need security. The purposes behind digital signatures are privacy and security, and a digital signature at first glance seems to fit the bill. The problem, however, is not the signature itself, but the lack of trust in a recipient. Impersonations become a looming security risk if you can't guarantee that the digital signatures you receive came from the people with whom they were supposed to have originated. For this reason, a certificate issued by a trusted third party provides the most secure authentication.

Q: Can I have a CA hierarchy that is five levels deep?

A: Yes, but that's probably overkill for most networks. Microsoft's three-tier model of root, intermediate, and issuing CAs will more than likely meet your requirements. Remember that your hierarchy can be wide instead of deep.

Q: Do I have to have more than one CA?

A: No. Root CAs have the ability to issue all types of certificates and can assume responsibility for your entire network. In a small organization, a single CA might be sufficient for your purposes. For a larger organization, however, this structure would not be suitable.

Q: How can I change the publishing interval of a CRL?

A: From the **Certification Authority** console, right-click the **Revoked Certificates** container and choose **Properties**. The **CRL Publishing Parameters** tab allows you to change the default interval for full and Delta CRLs.

Q: Why can't I seem to get autoenrollment for user certificates to work?

A: Remember that autoenrollment for machines is a feature that has been around since Windows 2000, but autoenrollment for user certificates is new to Windows Server 2003. In order to use this feature, you need to be running either a Windows Server 2003 or XP client and you must log on to a Windows Server 2003 domain. Finally, autoenrollment must be enabled through Active Directory's group policy. Also, you won't be able to autoenroll a user unless the user account has been assigned an e-mail address.

Q: What is the default validity period for a new certificate?

A: The default, which can be changed on the **General** tab of a new template's **Property** sheet, is one year. Other important settings, such as minimum key size and purpose of the certificate, can be found on the sheet's other tabs.

Q: If my smart card is lost or stolen, can I be reissued one?

A: Yes. The enrollment agent can enroll a new card for you at the enrollment station. Although most smart card providers allow cards to be reused (such as when they are found), a highly secure company may require old cards to be destroyed. For similar security reasons, PINs should not be reused on a newly issued card although it is possible. Remember that a card is only good to a thief if the corresponding PIN is obtained as well.

Q: When setting up smart cards for my company, can I use the MS-CHAP or MS-CHAP v2 protocols for authentication?

A: No. EAP is the only authentication method you can use with smart cards. It is considered the pinnacle of the authentication protocols under Windows Server 2003. MS-CHAP v2 is probably the most secure of the password-based protocols, but still does not provide the level of protection that smart cards using EAP do. This is because EAP is not really an authentication protocol by itself. It interfaces with other protocols such as MD5-CHAP, and is therefore extremely flexible. As a result it has been widely implemented by many different vendors. MS-CHAP and MS-CHAP v2 are Microsoft proprietary, and do not enjoy the same popularity or scrutiny applied to EAP. It is this scrutiny over the last several years that gives EAP the reputation of a highly secure protocol.

Q: How can I determine the length of time for which a certificate should be valid?

A: It is important to plan out your PKI implementation before it goes into production. In the case of certificate validity, you'll want to choose a time period that will cover the majority of your needs without being so long as to open your environment up to compromise.

If you are planning a certificate to support a traveling workforce that only connects to the corporate infrastructure once a quarter, it would be detrimental to expire certificates once a month. At the same time, specifying a certificate to be valid for 20 years might open your business up to compromise by an ex-employee long after his employment has been terminated.

Finally, you will want to ensure that your certificate lifetime is less than the lifetime for the lifetime of the CA's own cert. If the issuing CA will only be valid for a year, having a subordinate cert that is good for 5 years will lead to problems when the parent authority is revoked.

Q: My domain has been active for some time, but I have only recently implemented a Certificate Authority in my domain. I am now getting messages that my Domain Controllers do not have appropriate certificates. What should I do?

A: Make sure that you have enabled auto enrollment on your Domain Controller certificate templates. This step is often missed and can lead to a number of secondary problems, the least of which is annoying messages in the Event Logs.

Self Test

1. You have been asked to provide an additional security system for your company's internet activity. This system should act as an underlying cryptography system. It should enable users or computers that have never been in trusted communication before to validate themselves by referencing an association to a trusted third party (TTP). The method of security the above example is referencing is?
 - A. Certificate Authority (CA)
 - B. Nonrepudiation
 - C. Cryptanalysis
 - D. Public Key Infrastructure (PKI)
2. You are engaged in an exercise that is meant to demonstrate the Public-Key Cryptography Standards (PKCS). You arrive at a portion of the exercise dealing with encrypting a string with a secret key based on a password. Which of the following PKCS does this exercise address?
 - A. PKCS #5
 - B. PKCS #1
 - C. PKCS #8
 - D. PKCS #9
3. You are working in a Windows Server 2008 PKI and going over various user profiles that are subject to deletion due to company policy. The public keys for these users are stored under Documents and Settings\Administrator\System Certificates\My\Certificates and the private keys would be under Documents and Settings\Administrator\Crypto\RSA. You possess copies of the public keys in the registry, and in Active Directory. What effect will the deletion of the user profile have on the private key?
 - A. It will have no effect.
 - B. It will be replaced by the public key that is stored.
 - C. The Private Key will be lost.
 - D. None of the above.
4. Two users, Dave and Dixine, wish to communicate privately. Dave and Dixine each own a key pair consisting of a public key and a private key. If Dave wants

Dixine to send him an encrypted message, which of the following security measures occurs first?

- A. Dave transmits his public key to Dixine.
 - B. Dixine uses Dave's public key to encrypt the message.
 - C. Nothing occurs the message is simply sent.
 - D. Dixine requests access to Dave's private key.
5. You are browsing your company's e-commerce site using Internet Explorer 7 and have added a number of products to the shopping cart. You notice that there is a padlock symbol in the browser. By right clicking this symbol you will be able to view information concerning the site's:
- A. Private Key.
 - B. Public Key.
 - C. Information Architecture.
 - D. Certificates.
6. You are engaged in an exercise that is meant to demonstrate the Public-Key Cryptography Standards (PKCS) used in modern encryption. You arrive at a portion of the exercise which outlines the encryption of data using the RSA algorithm. Which of the following PKCS does this exercise address?
- A. PKCS #5
 - B. PKCS #1
 - C. PKCS #8
 - D. PKCS #9
7. You are the administrator of your company's Windows Server 2008-based network and are attempting to enroll a smart card and configure it at an enrollment station. Which of the following certificates must be requested in order to accomplish this action?
- A. A machine certificate.
 - B. An application certificate.
 - C. A user certificate.
 - D. All of the above.
8. Dave and Dixine each own a key pair consisting of a public and private key. A public key was used to encrypt a message and the corresponding private

key was used to decrypt. Dave wants Dixine to know that a document he is responding with was really written by him. How is this possible using the given scenario?

- A. Dave's private key can encrypt the document and the matching public key can be used to decrypt it.
 - B. Dave can send Dixine his private key as proof.
 - C. Dixine can allow Dave access to her private key to encrypt the document.
 - D. None of the above.
9. You are administrating a large hierachal government environment in which a trust model needs to be established. The company does not want external CA's involved in the verification process. Which of the following is the best trust model deployment for this scenario?
- A. A hierachal first party trust model.
 - B. A third party single CA trust model.
 - C. A first party single CA trust Model.
 - D. None of these will meet the needs of the company.
10. Two users, Dave and Dixine, wish to communicate privately. Dave and Dixine each own a key pair consisting of a public key and a private key. A public key was used to encrypt a message and the corresponding private key was used to decrypt. What is the major security issue with this scenario?
- A. Private keys are revealed during the initial transaction.
 - B. Information encrypted with a public key can be decrypted too easily without the private key.
 - C. An attacker can intercept the data mid-stream, and replace the original signature with his or her own, using his private key.
 - D. None of the Above.

Self Test Quick Answer Key

- | | |
|------|-------|
| 1. D | 6. B |
| 2. A | 7. C |
| 3. C | 8. A |
| 4. A | 9. A |
| 5. C | 10. C |

Chapter 8

MCITP Exam 647

Planning for Server Virtualization

Exam objectives in this chapter:

- Understanding Windows Server Virtualization and Consolidation Concepts
- Learning to Install and Configure Windows Server Virtualization
- Learning about System Center Virtual Machine Manager 2007
- Learning to Manage Windows Server Virtualization-Based Assets

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

Although the concept of virtualization has been around since the early days of computing, the technology has only recently come into its own on a large scale. This has happened not only as a result of dramatic improvements to the technology itself, but also due to vast and rapid improvements to supporting hardware technologies such as memory and disk storage density.

As well this new supporting hardware is becoming available at ever increasing levels of affordability, meaning that IT managers are finding it that much easier to rationalize the business arguments behind the large-scale shift toward the deployment of virtualization technology into their data centers. This is especially true in larger enterprise environments where the cost savings realized by the deployment of virtualization solutions are most significant. Forward-thinking managers can easily see the inherent value in a move to virtualize any and all IT assets that fit the appropriate criteria.

The potential benefits of server consolidation alone are difficult to ignore, but when coupled with other advantages, such as the additional benefits of improved efficiency in administrative efforts, streamlined processes and procedures, virtualization can quickly become much less of an option than a requirement for companies constantly searching for new ways to control costs, and remain competitive in today's business climate. Beyond the cost benefits, for IT administrators struggling with the ever-increasing problem of task and information overload, the improvements in efficiency, process and procedures made possible by the advent of virtualization have become a welcome addition.

Understanding Virtualization

Server virtualization is a technology that allows many autonomous operating systems to use the same physical hardware while running in isolation from one another. This technology allows for the creation of a layer of isolation between the operating system of each individual virtual machine (VM) and the physical hardware below them. The layer of isolation allows for the emulation of the presence of actual physical hardware within each virtual machine. The end result being that each individual virtual machine runs as though it were actually running on physical hardware.

This technology has matured significantly in recent years, to the point where its large-scale use has become practical on many levels. In fact there has been an ever-increasing trend toward the widespread proliferation of this technology, and there appears to be no end in sight. Looking toward the future, Microsoft has aggregated

its vision for the use of virtualization technology into three main directions. These would be the server, application, and presentation virtualization. For the moment we'll focus on the server virtualization solution, while touching on the other solutions later on in the chapter.

There are several key benefits, as well as potential issues to be considered with a migration to virtualization technology. For most organizations the benefits far outweigh any potential issues, but just the same all factors must be considered equally and fully. The key benefits include the following:

- **Greatly improved efficiency** with respect to the resource utilization of available IT assets.
- **Highly effective and dynamic adjustments** Available tools for the centralized management of virtual assets allow for highly effective and dynamic adjustments to be made to the resource consumption of each individual virtual machine.
- **One Common Management Interface** What this means is that instead of having hundreds of physical servers running in a data center often at very low levels of utilization, it is possible to view and assess large numbers of virtual servers through one common management interface.
- **Optimize the distribution of available resources** This common management interface also allows administrators to make fast, easy, and efficient adjustments to the levels of processor, memory, and disk storage space resource utilization in order to optimize the distribution of available resources. Something that has never before been possible on an enterprise level.
- **Maximum density of virtual capacity** The obvious advantage is that with a minimum amount of administrative effort each individual virtual machine can be tuned to use exactly the correct amount of resources that it requires, and nothing more. This allows for maximum density of virtual capacity to be used and maintained, eliminating the old problem of wasted data center capacity.
- **Greatly reduced wastage** Greatly reduced wastage of data center space, power consumption, and cooling capacity.
- **Fewer physical servers** The application consolidation and densification with the deployment of virtualization technology within the data center means that fewer physical servers are required to accomplish the same workload.

- **Lower consumption of supporting resources** Fewer servers result in lower consumption of supporting resources.
- **Improved response times** Vastly improved response times to business requirements.
- **Adjust and adapt more easily** Since administrative and development staff are able to adjust and adapt to current conditions much more easily and effectively than was previously possible. This means that business requirements can be met much more quickly and accurately than was previously possible.
- **Servers deployed in a fraction of the time** Beyond the ability to adapt to resource utilization requirements, the ability to deploy new virtual servers, relocate them as needed, as well as recover from problems allowing replacement virtual servers to be brought online in a fraction of the time that was previously possible also means that business requirements are not only met, but maintained much more quickly and effectively.

Potential issues to be considered when implementing virtualization include the following:

- **Management of virtual assets** How to effectively safely integrate the management of virtual assets together with existing non-virtual IT assets.
- **Continuity between physical and virtual assets management** The proper selection, evaluation, and eventual investment of the right management tools is a critical decision and will directly affect the eventual success of any large-scale deployment of virtualization technology into an organization's IT infrastructure. Whatever tools are chosen, it is important that they integrate well across both virtual and physical platforms, and provide an acceptable degree of continuity between the management of physical and virtual assets.
- **Too many different management tools** The selection of many different tools for each individual requirement will result in a disjointed solution resulting in administrative inefficiencies and oversights. Too many different tools that are not well integrated with one another will increase not only IT administrative workload but also the chances that critical issues will be overlooked by IT administrators left to sort through large amounts of potentially conflicting and confusing information.

- **Risks from the introduction of a new technology** How to avoid the risks to application availability caused by the introduction of a new technology into the IT infrastructure of an organization.
- **The learning curve** With the deployment of virtualization technology into an organization's infrastructure, there is always a risk to the availability of IT resources caused by the lack of experience with that technology in the early stages. The learning curve, as it is often called, presents a very real risk to an organization's environment that needs to be considered during deployment. IT managers can mitigate this risk to a degree through effective training and information sharing policies; but in the end there is no substitute for real-world experience.
- **Properly identify and validate suitable workloads** How to properly identify and validate which physical server workloads are suitable for migration to a virtual platform, and which are not.
- **Process and standards must be developed** Not all server workloads can or should be virtualized. Processes and standards must be developed within any organization to properly assess and identify which workloads are acceptable candidates for migration to a virtual platform.
- **Generally not good candidates** As a starting point, workloads that are deemed as mission critical are generally not good candidates for virtualization. A server should not be virtualized unless it is running a function that could potentially tolerate an unanticipated outage.
- **Virtual platforms may go down unexpectedly** While great gains have been made in the development of high-availability solutions for virtual platforms, there is still an element of risk that virtual platforms may go down unexpectedly for a wide variety of reasons.

Server Consolidation

When individual servers are utilized in support of each individual application required within an organization, there is always an unavoidable degree of inefficiency and wastage that results from the inevitable underutilization of these hardware resources. It is difficult to effectively plan for true resource utilization when using physical servers since these servers are by their very nature somewhat static and difficult to adapt to individual circumstances and requirements of each individual application and its resource requirements. While it is true that memory and disk space can be added to physical servers as required, the limitations are more centered around the inability to

accurately and dynamically identify which physical servers are overutilized, and which are underutilized from the enterprise perspective. For the most part hardware is often ordered and deployed on the too-much-is-better-than-not-enough-resources philosophy, meaning that many data centers are left running large quantities of servers that are hugely underutilized. Although somewhat unavoidable with conventional server technology, this situation unfortunately results in large-scale wastage of power, cooling, and space. In fact many servers may often be running at extremely low resource utilization levels, resulting in significant wastage of precious data center resources. Power consumption, data center floor space, as well as administrative effort are wasted in this scenario due to the inefficient and inexact allocation of resources to the individual needs of each resident application. It is for this reason, amongst others, that the server consolidation allowed by virtualization technology is so attractive enterprise environments trying to control costs, improve efficiency, and remain competitive.

The application of virtualization to this issue allows for multiple server roles to be consolidated onto one or at least fewer virtual server workloads. There is a balance to be maintained in this process between maintaining required levels of separation between specific server roles, and their associated workloads that require redundancy, and obtaining an optimized level of resource utilization. For the most part, it is not wise to consolidate certain functions whose roles are either of critical importance to the organization, since maintenance activities in one role could adversely affect another. Sometimes functionalities need to be maintained on separate workloads in order to ensure their availability throughout the enterprise. It is however still feasible and beneficial to consolidate multiple server roles on to multiple separate virtual machines, provided that they are kept on separate physical hosts. This is an acceptable way to achieve the desired server and data center densification with all of its positive effects while still maintaining the layers of separation necessary to guarantee functionality and availability of key resources. The key is in the proper selection of acceptable candidates for consolidation on to virtual platforms. Not all server workloads are well suited for this transition.

Quality Assurance and Development Testing Environments

The application of virtualization technology to the process of lab environment creation has dramatically improved the flexibility and adaptability of these environments to the needs of IT resources that depend on them for their everyday requirements. The ability to recreate and or copy development servers running on virtual platforms in minutes rather than hours or even days that it used to take

before virtualization technology was available is invaluable. In addition, virtual machines can have their present state backed up very quickly by means of snapshots or file copies, which allow administrators or developers to recover very rapidly from problems or changes that didn't behave as expected. This means that they can spend their time more effectively on troubleshooting what went wrong, rather than wasting time on rebuilding or reinstalling applications and operating systems after undesirable test results have corrupted or compromised their state. Inevitably time is money, so the investment in virtual technology for the laboratory environment is one that unquestionably pays off many times over in reduced reaction times to problem resolution as well as overall improved IT resource utilization.

Before virtualization, a developer would be limited to a process of allocating available physical hardware, securing the physical space and power required to host that physical hardware, and then building up the required operating system and application base to support his or her testing needs. Often this required multiple servers all interacting on a dedicated network segment in order to accommodate and replicate all of the individual functionalities that the developer might require. Supporting functionalities such as a replicated copy of the production Active Directory database running on a lab-based domain controller to provide authentication and permissioning within the lab environment are a common requirement that demand a greatly increased input of time, effort, and physical resources from the lab's constructor.

In the days before virtualization technology had matured sufficiently to be used effectively for this purpose, re-creating a copy of the production Active Directory database in a lab environment was a tricky process that required specific skills and experience, as well as a detailed knowledge of the inner workings of Active Directory. With the introduction of virtual technology into this scenario, a detailed knowledge of Active Directory's inner workings is still required; but the actual process of transplanting a working copy of Active Directory into an autonomous laboratory environment to support the requirements of testing in that environment has become dramatically less complicated. All that is required to facilitate this procedure is one production domain controller running on a virtual server platform that can be quickly and easily shut down in order to allow its .vhf file to be copied. A new blank replacement version of the virtual production domain controller can then be recreated on a different host in the laboratory environment. During the new VM-creation process, the new VM is configured to use the transplanted .vhf file as its virtual disk. The new VM can then be started and will run as a perfect copy of the original. There are other configuration tasks and requirements involved with this procedure, but they are beyond the scope of this text.

Head of the Class...

New, Previously Nonexistent Threats to Both Security and Stability

Be advised that although the introduction of virtualization technology into the scenario of lab creation has allowed for this common requirement to be much more easily fulfilled, it has also had the unintended side affect of introducing new, previously non-existent threats to both the security and stability of the production Active Directory environment that must be considered and taken seriously.

Security Risk The ability to quickly and easily copy a .vhdx file from a domain controller residing in the production environment on to portable media and transport that file into a lab environment for the purpose of replicating Active Directory's functionality has, without question, been a boon to all those who seek to build such lab environments. Unfortunately it has also made it dramatically easier for someone with malicious intent to transfer that copied file onto any one of a multitude of forms of portable media available today, and walk out the door with it, right under the unsuspecting noses of the many levels and layers of physical- and network-based security that so many companies have spent vast amounts of time and money to implement. I have all too often seen companies whose IT staff focus so much effort on making their environments as secure and protected as possible, yet they overlook this simplest method of bypassing all that security in a matter of minutes. All it takes is a memory key with sufficient capacity to hold a .vhdx file in the hands of someone with the intent to use that information for other than legitimate purposes. Many companies have taken steps via modern resource monitoring solutions to prevent such attempts at critical file copies from being carried out without being noticed in their production environments, yet do not employ the same level of protection and monitoring in their laboratory environments. This makes the lab-based copy of Active Directory an easy target and, therefore, the most reasonable place for someone seeking to obtain this information to go. One quick file copy and this person has all the password and permissions information for every single person, from the mail clerks to the CEO. It is, therefore, strongly recommended that this significant threat to any organization's network security not be taken lightly.

Continued

Stability Risk It is a very common requirement for the users of any such laboratory environment to request that remote connectivity to this environment be made available throughout the enterprise in order to allow for distributed access for users who are often geographically dispersed. This geographical dispersion is a common scenario in modern companies, which often makes the exposure of such a lab to the main production environment for administrator or developer access purposes more of a core requirement than a luxury. This requirement would most commonly be accomplished through the use of a firewall that is configured to block all Active Directory-related network communication, allowing for nothing more than the remote connectivity functionality that is required. I have seen this configuration successfully implemented on many occasions; however, having had a great deal of experience in this area I would warn that Active Directory responds very negatively to exposure to an exact copy of itself. When confronted with a mirror image of itself, Active Directory immediately goes into conflict resolution mode, deciding for itself which duplicate domain controllers are real, and which are not. In other words, you could suddenly find your enterprise authenticating to your tiny little lab, and the state of your Active Directory database in a complete mess in the wake of an event such as this. There are many circumstance-specific details that would greatly affect the real-world results of an event like this. It is enough for our purposes here, though, to say that a mistake made during the configuration of this sort of lab setup in a large multisite enterprise environment has the very real potential to be nothing less than devastating. For this reason, I would strongly recommend that significant attention and respect be given to the prominent labeling and documentation of any cabling and specific configurations made in support of any lab environment containing an exact copy of any company's production Active Directory database. The prominent display of labeling and documentation is critical as memories will fade with time passed since initial configuration, or people originally involved may move on to other opportunities. Over time it would be very easy for some unsuspecting individual to move a cable or reconfigure the firewall and unwittingly cause a devastating outage. For this reason, it is also strongly recommend that this serious threat to domain stability not be taken lightly.

Disaster Recovery

The traditional way of recovering from unexpected events, involving the time-consuming process of rebuilding servers manually, and then restoring files from backup can be nothing less than painful. This is especially true when there is

often considerable pressure from business users and management to accomplish the task much faster than previously available technologies allow for. For many larger organizations, the requirement to maintain dedicated disaster recovery sites with duplicated hardware and applications, is expensive, inefficient, and labor-intensive.

There are a wide variety of ways in which virtualization technology could be applied in an organization's disaster recovery planning process. While it is true that virtualization cannot be looked at as the one answer to all disaster recovery needs, it can certainly be utilized to lower the associated costs and reduce the administrative burden of maintaining a disaster recovery. Most importantly, it can allow an organization to recover more quickly and efficiently in the event of an expected event.

The fact that virtual disk files can be quickly and easily moved from one dissimilar hardware platform to another with no effect to the actual virtual server itself offers organizations a great deal of flexibility in how this technology can be used to protect themselves against unforeseen catastrophes. Additionally, the virtual machine snapshot capability included with the Windows Server virtualization model provides options for the rapid recovery from a multitude of differing situations.

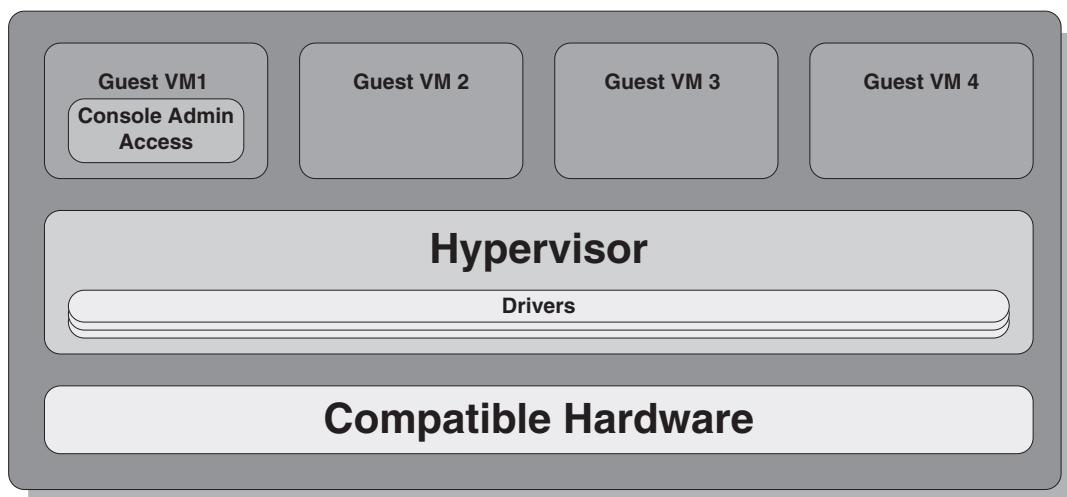
Microkernelized vs. Monolithic Hypervisor

Previous iterations of virtualization technology have utilized monolithic-style hypervisor technology. Valued for its good performance characteristics, monolithic hypervisor has allowed virtualization technology to progress to the level that has made large-scale proliferation into the IT marketplace that it now enjoys possible. Unfortunately, there are now ever-increasing threats to any company's IT resources, largely in the area of security, that have made it necessary to look beyond the scope of pure performance towards other requirements. Not the least of which is the need to maintain an environment that has a reduced level of vulnerability to attack from hackers and their instruments of attack that have become so pervasive in the world of IT.

Monolithic Hypervisor

Monolithic hypervisor runs the drivers required to access and control the underlying hardware within itself. This means that the hypervisor layer is actively involved in the process of providing hardware connectivity and awareness to the virtual machines running above it. The configuration allows the virtual machines to run in the hypervisor layer above as if they were actually running on physical hardware. One of the guest operating systems above would traditionally be used to provide the needed access to the console and its associated management tools used to administer the virtual environment (see Figure 8.1). This configuration has its advantages as well as some key disadvantages.

Figure 8.1 Monolithic-Style Hypervisor Architecture



Some key advantages are:

- **Performance characteristics** The monolithic hypervisor design is valued for its performance characteristics.
- **Support for guest operating systems** The monolithic hypervisor design is also valued for its ability to provide support to a wide range of guest operating systems.

Some key disadvantages are:

- **An easy point of attack for hackers** The monolithic hypervisor design provides an easy point of attack for hackers. The fact that the monolithic Hypervisor runs device drivers within its own layer of functionality means that it becomes an attractive point of attack for those people with intent to do harm to a company's network resources. This style of architecture provides an opportunity for the hacker community to embed malicious code into software that would traditionally be run in the hypervisor layer on virtualization platforms that utilize the monolithic hypervisor-type design. Such malicious code, once present in the hypervisor layer, would then provide the means to compromise the security of all virtual machines running above the hypervisor layer, greatly enhancing the hacker's potential impact over the old style individual server by server attack.
- **More susceptible to instability** The monolithic hypervisor design also leaves it more susceptible to instability caused by driver issues. The fact that

the monolithic hypervisor runs device drivers within its own layers of functionality means that it is also susceptible to instability caused by any issues with those drivers. This means that every time a system driver is updated or rewritten, potential code bugs or faults in such newly-written software present a risk to the entire underlying structure of the virtual environment. Therefore, instead of a new driver potentially destabilizing only one operating system at a time, the new driver can now potentially destabilize all of the virtual machines running on any one unit of physical hardware.

Microkernel Hypervisor

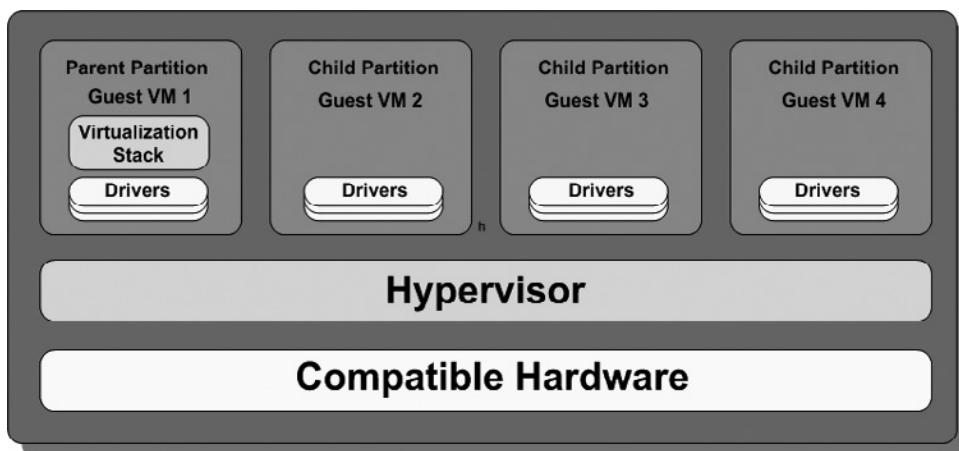
The microkernel-style of hypervisor architecture removes device drivers from the hypervisor layer entirely (see Figure 8.2). The drivers have been relocated to the individual guest operating system partitions, where they run separately for each individual virtual machine. This is the type of hypervisor technology that is utilized by Windows Server 2008.

These separate partitions are the method of isolation utilized by the microkernel hypervisor. The first partition is the parent partition, which not only contains the virtualization stack, but also the tools and functionality needed to create and control the subordinate child partitions.

The virtualization stack sits on top of the hypervisor in the parent partition, and performs all virtualization functionality for the virtual machines beyond what the hypervisor itself is intended to do.

The parent partition also provides access, via WMI to any third-party management tools that can be used to manage the virtual machines running in the child partitions.

Figure 8.2 Microkernel-Style Hypervisor Architecture



As was the case with monolithic hypervisor, microkernel hypervisor also has its advantages and disadvantages. Some key advantages are:

- **Reduced vulnerability to security invasions** It reduces the vulnerability to security invasions within the hypervisor layer caused by the potential threat from malicious code being embedded in driver software. This means that hackers no longer have the ability to compromise multiple virtual machines with one attack. They are once again limited to one-by-one-style attacks on individual virtual machines running above the hypervisor layer.
- **Removes the vulnerability to system destabilization** It removes the vulnerability that the entire system and all virtual machines running on it can potentially be destabilized by any software code errors contained in newly introduced system drivers. Since the drivers run at the virtual machine level above the hypervisor level, any potential driver issues would affect the individual virtual machines on a one-by-one basis. This greatly reduces the overall risk of destabilization to the entire virtual environment.
- **Removes tried and tested drivers will continue to work** Since the drivers run at the operating system level, there is no need to create new drivers to work with the new style of hypervisor technology. This also greatly reduces the risk to dependant systems because tried-and-tested drivers will continue to work just the same as if they were being utilized in a non-virtualized environment.

A key disadvantage is:

- **Reduced performance** It has slightly reduced performance from the monolithic hypervisor model.

Detailed Architecture

The type of technology utilized to accomplish the Windows Server 2008 Hyper-V method of virtualization is hardware-based and, therefore, requires the support of 64-bit processors that contain specific functionality improvements designed to work in conjunction with Windows Server 2008 to achieve the desired performance and functionality.

First, this is because the design of the microkernel hypervisor requires the assistance of the processor to facilitate certain portions of the communication between the virtual machines and the underlying physical hardware.

Second, these processors and their specific functionality are required for a function called Data Execution Prevention (DEP). This is a security feature that Intel has labeled XD (eXecute Disable) and AMD refers to as NX (No eXecute). The Data Execution Prevention feature has been an included component in every version of Windows since Windows XP SP2, but it has been elevated to a mandatory prerequisite for the installation and running of the Hyper-V Role in Windows Server 2008. Its purpose is to block the execution of malicious code by segregating memory into separate areas for processor-related functions and data storage. This serves to provide barriers to common exploits that use buffer overflows to store and run malicious code in memory. While there is a slight performance loss to guest VMs, Microsoft has decided that this loss is worth the hit in order to maintain a secure platform for their Hyper-V-based virtual machines.

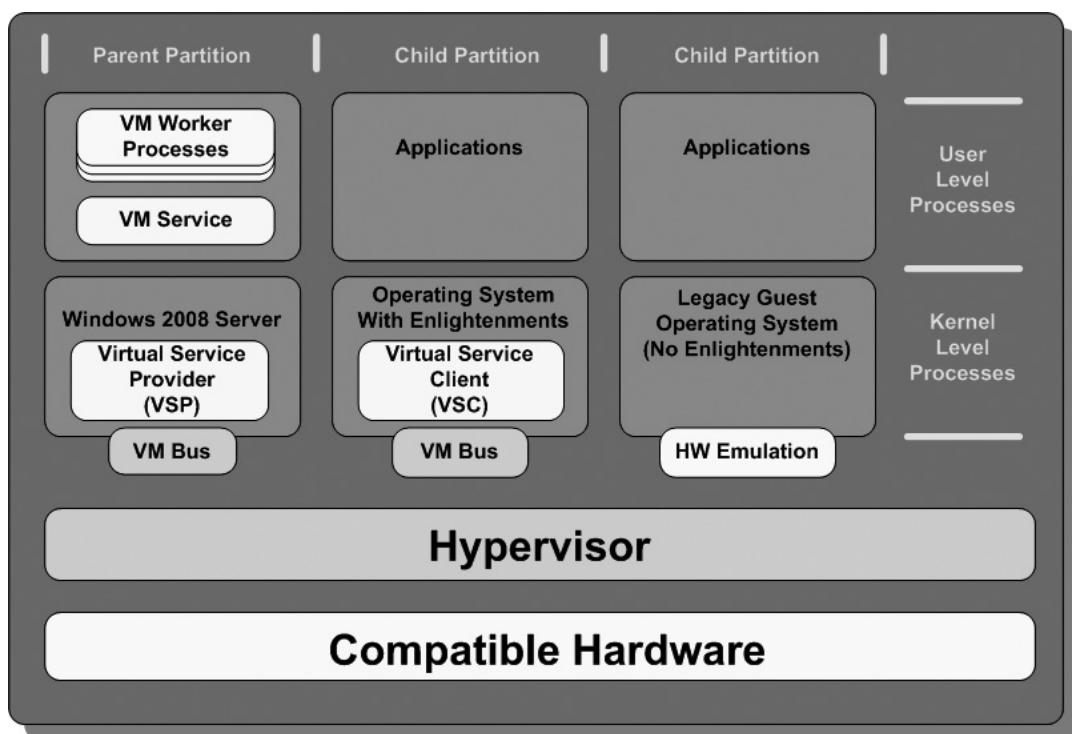
Specifically, the processors required to support these functions are the AMD-V or Intel VT processors. There are detailed vendor-specific listings available showing exactly which processors from each manufacturer will support this functionality; therefore, it is imperative that these references be consulted to ensure compatibility before purchasing hardware with the intent to deploy Window 2008 Server virtualization.



TEST DAY TIP

Not only is it imperative that the latest version of BIOS be verified to be installed, but also the needed features must be enabled within the BIOS in order to ensure the proper operation of hardware-assisted virtualization. If these features are not enabled in the BIOS, Hyper-V will not start after installation.

In Windows Server 2008-based virtualization architecture, individual guest operating systems are not only isolated by physical partitions but also subdivided by kernel and user process levels (see Figure 8.3).

Figure 8.3 Virtualization Architecture in Windows Server 2008

Parent Partition

The parent partition is where an instance of Windows Server 2008 will be installed. This can be either a full install of Windows Server 2008 or just a server core installation. It is highly recommended that this installation be restricted to a server core installation. This is for two reasons:

- **Less susceptible to security related attacks** A server core installation of Windows Server 2008 provides a platform for virtualization that is less susceptible to security-related attacks because only the minimum required services, ports, and resources are utilized to accomplish the necessary functionality. Fewer services enabled and ports opened means that hackers have fewer points of attack with which to work.
- **More resources available virtualization processes** Fewer services and resources are utilized by a Server Core installation of Windows Server 2008 means that more of the hardware's underlying resources are left available for use by virtualization processes.

The Windows Server 2008 instance in the parent partition is separated by two process levels, Kernel Mode Processes and User Mode Processes.

The Kernel Mode segment of the parent partition contains, and runs three components:

- The Windows kernel of the parent partition's guest operating system
- Virtualization Service Provider or VSP
- The VMBus

While previous iterations of virtualization technology utilized hardware emulation to provide access to hardware for guest operating systems, Windows Server 2008 utilizes the Virtualization Service Provider (VSP) to accomplish this functionality. The job of the VSP is to talk to the device drivers and act as a proxy service to satisfy the hardware-access requirements of the other guest operating systems running in the child partitions. The VSP is a key part of what allows Windows Server 2008 Virtualization to work. The VSPs form pairs with their corresponding Virtualization Service Clients (VSCs) running in the child partitions, mentioned later.

The device emulation method used in previous versions on virtualization technology allows for a high level of compatibility with multiple operating systems, both legacy and new. Unfortunately, this benefit of compatibility comes at the cost of providing poor performance for guest operating systems running on this type of platform.

The job of the VMBus is to provide a conduit over which requests and data can be sent between guest virtual machines. The previously mentioned VSP/VSC pairs of Virtual Service Providers from the parent partition and their corresponding Virtual Service Client components running in the child partitions utilize the VMBus to accomplish their required communication.

The User Mode segment of the parent partition also contains, and runs three components:

- **Virtual Machine Service (VMS)** Provides access to the management of virtual machines and their worker processes.
- **Virtual Machine Worker Processes** Run within the virtualization stack and supports each VM separately. Also, each VM has its own Virtual Machine Worker Process.
- **The WMI Provider** Provides interfaces for the management of virtualization.

Child Partitions

As was the case with the guest operating system running in the parent partition, the processes within the child partitions are also separated into kernel mode processes and user mode processes.

In the child partitions there are two key components that run in kernel mode:

- Guest operating system component of the virtual machine
- Virtual Service Client (VSC)

The Virtual Service Client works together with the Virtual Service Provider from the parent partition to provide the main path of communication for all system-related traffic. There is one VSP/VSC pair created for each device type within the system.

Requests for resources from the application layer of a virtual machine running at the User Mode level are passed to Virtual Service Client running at the Kernel Mode level of an enlightened operating system child partition.

The Virtual Service Client then passes this resource request to its corresponding Virtual Service Provider running in the parent partition's operating system. That Virtual Service Provider then actions the request, and allows the appropriate resource to perform the desired action.

The User Mode segment of the child partition is where installed applications are run on the guest virtual machines.

Guest Operating Systems

There are three main categories of guest operating systems that can be run in the child partitions of a Windows Server 2008 virtual platform:

- Guest with enlightened operating system
- Guest with a partially enlightened operating system
- Legacy guest operating system or guest without enlightenments

Guest with Enlightened Operating System

In general, a guest operating system that would be classified as enlightened is one with specific enhancements that allow it to be fully aware that it is running in a virtual environment. This enhanced functionality and awareness allows these guest operating systems to utilize a fully-optimized virtual interface using no emulation for hardware communications.

A common example of operating systems that fit these criteria would be one of the following:

- Windows Server 2008.
- Windows Vista and Windows XP SP3.
- SuSE Linux Enterprise Server 10 with Service Pack 1 (x86 and x64 editions).
- **Xen-Enabled Linux Kernels** Citrix worked together with Microsoft to develop software that would translate XenServer's virtualization communication format into one that could be read by Hyper-V's virtualization engine. The result is a thinlayer software called the **Hypercall Adapter**. This software allows Xen-enabled Linux Kernels to run on the Hyper-V platform, and take advantage of the performance advantages available to the other enlightened guests identified above.

Guest with Partially Enlightened Operating System

A guest operating system that is partially enlightened requires the assistance of hardware emulation in order to accomplish some hardware communications, but does have some driver-specific enlightenment capabilities.

An example of a partially enlightened guest operating system would be Windows Server 2003.

Legacy Guest

A legacy guest operating system is one that has been written to run on physical hardware, and has no capability at all to be aware of the fact that it might be running on a virtual platform. This type of operating system requires the full support of emulation in order to communicate with the underlying hardware and function as desired.

This emulation is not included in the hypervisor's functionality and must be provided by an external monitor. The use of emulation in this scenario is substituted for the Virtual Service Client functionality; therefore, legacy guest operating systems do not use the VSC component of Windows Server 2008 Virtualization.

Application Compatibility

Virtualization technology also provides a means to work around issues of application compatibility. As organizations inevitably upgrade their infrastructures in order to take advantage of the benefits of available new technologies with their increased functionality and improved security, there will always be applications that do not conform to the criteria imposed by the upgraded environments in which they may

be forced to exist. When an IT organization upgrades its infrastructure to the next generation of Windows Server platform, for instance, the infrastructure components of that organization such as Active Directory Services, DNS, DFS will most often present the least amount of technical resistance to that upgrade effort.

The application base of such an organization can often be a very different story. The complications surrounding application compatibility with increased security both at the operating system and network infrastructure level can create a long list of compatibility issues that must be solved in order to keep such an organization running. In many cases the answer is to upgrade the applications to a newer version that is compatible with the new standard, but this can often prove to be impractical, if not even impossible. Especially in larger organizations that may be running applications numbering in the hundreds or even thousands, the shear cost of such upgrades can easily exceed acceptable levels. For many organizations, the associated cost of achieving true application compatibility can be much more of a limiting factor than the complexity of meeting this goal.

The application of virtualization technology to this problem can provide acceptable work-arounds to these sorts of issues in many ways. For instance, an application that requires the presence of a legacy operating system or other legacy version of a dependant infrastructure component can be installed on a virtual platform that can be run autonomously on top of the updated operating system, allowing for the co-existence of the two differing levels of technology via the same access point (workstation, and so on). This sort of arrangement allows for greatly increased flexibility when it comes to the provision of necessary services and applications to the end users in an organization.

Microsoft Server Virtualization

Virtual Server 2005 R2 utilizes an application-based virtualization model. It is designed to be installed, and run as an application on top of an Operating System. The main operating system intended for host support of Virtual Server 2005 R2 is Windows 2003 SP2, but it will run on all 32-bit versions of Windows 2003 Server.

NOTE

Virtual Server 2005 R2 SP1 is a requirement in order to run on any 64-bit host operating system. Pre-SP1 versions will run on 64-bit hardware provided that the operating system is a 32-bit version.

Windows XP Professional is also supported as a host operating system, but it is not recommended for any use other than for testing and development purposes.

Virtual Server 2005 is available in two versions:

- **Virtual Server 2005 Standard Edition** Virtual Server 2005 Standard Edition can run on a host with a maximum of four processors.
- **Virtual Server 2005 Enterprise Edition** Virtual Server 2005 Enterprise Edition can run on a host with four or more processors. Maximum number of processors is determined by the host operating system.

Virtual Server 2005 R2 utilizes emulation technology in order to provide virtualization services to its guest virtual machines. As stated in the previous section on Windows Server 2008 Virtualization architecture, the emulation method of providing virtualization services has some key benefits as well as some drawbacks.

The main benefit provided by the use of emulation technology overall is that it provides the ability to offer widespread compatibility to a long list of guest operating systems. Both the newer generations of operating systems (O/Ss) as well as many legacy O/Ss run equally well on the emulated hardware platform.

Here is a list of supported guest operating systems:

- Windows Server 2008 Standard and Enterprise
- Windows Server 2003 Standard, Enterprise, and Web
- Windows SBS 2003 Standard and Premium R2
- Windows 2000 Server and Advanced Server
- Windows Vista Ultimate, Business, and Enterprise
- Windows XP Professional

Here is a list of supported non-Windows guest operating systems:

- Red Hat Enterprise Linux 2.1 (7), 3.0 (8), 4.0 (4)
- Red Hat Linux 9.0
- SuSE Linux Enterprise Server 9.0 and 10.0
- SuSE Linux 9.3, 10.0, 10.1, and 10.2
- Solaris 10
- OS/2 4.5

Although Virtual Server 2005 R2 does have the capability to support a wide range of guest operating systems, there are limitations to its capabilities which mostly result from its use of emulation technology. The single biggest drawback of this technology is poor performance for the hosted virtual machines.

Another key benefit that was added with the introduction of the R2 release of Virtual Server 2005 was support for PXE boot. This important functionality allows for the network-based deployments of operating systems to virtual machines via automated deployment solutions such as RDP. This is a functionality that is often a heavily used option by administrators for the management of virtual environments. USB support is currently limited to keyboard and mouse devices.

The introduction of SP1 has advanced the functionality of Virtual Server 2005 significantly, bringing its capabilities somewhat closer in comparison to that of the newer Windows Server 2008 Virtualization model. While Virtual Server 2005 may not have the power and capability of the newer virtualization model, its improved capabilities will allow it to be more readily utilized in partnership with the newer technology, easing the transition from the old to the new. In this manner, existing environments that have been built on virtual server technology can be upgraded to Windows Server 2008 Virtualization platforms over a period of time, preventing the wastage of previous efforts.

There are several functionality upgrades to Virtual Server 2005 R2 technology with the introduction of SP1. Some examples of the most significant improvements are as follows:

- **Support for hardware assisted virtualization** Virtual Server 2005 R2 SP1 can now utilize Intel V and AMD V generation processor support, meaning that it can be run on the same class of hardware as Windows Server 2008 Virtualization. This is a significant advancement that not only allows for the utilization of superior hardware platforms, but also for the deployment on Virtual Server 2005 on 64-bit versions of host operating systems.
- **Support for up to 256Gb of memory** Virtual Server 2005 R2 SP1 can now utilize up to 256Gb of memory. To use this option it is necessary to enable the Physical Addressing Extensions (PAE) switch on the host operating system.
- **Support for an Increased Number of Guest Virtual Machines** Virtual Server 2005 R2 SP1 can now support up to 512 guest virtual machines on 64-bit hosts. It can still only support up to 64 virtual machines if they are running on a 32-bit host. This remains unchanged from the pre-SP1 release.

- **Support for Windows Vista** Windows Vista is now included as a supported host operating system. The pre-SP1 release supported Windows XP SP2 as a host O/S. Windows Vista and Windows XP are intended for non-production use only, such as development and testing environments.

Virtual Server 2005 R2 utilizes a browser-based administrative Web site as the main point of administrative control over the virtual environment (see Figure 8.4). The management interface provided here is simple and straightforward to use. The functionality and features are somewhat limited in comparison to other virtualization solutions available on the market today, although the Virtual Server Migration Toolkit (VSMT) does support the important P2V migration capability for Virtual Server 2005 R2.

Figure 8.4 Virtual Server 2005 R2 Administration Web Site

The screenshot shows a Microsoft Internet Explorer window with the title "Virtual Server 2005 R2". The address bar contains the URL "http://Server2008/VirtualServer/VSWebApp.exe/viewer". The left sidebar has a navigation menu with options like Master Status, Virtual Server Manager, Virtual Machines, Virtual Disks, Virtual Networks, and Virtual Server. The main content area displays a table titled "devad3.rci.rogers.ca Status" with columns: Remote View, Virtual Machine Name, Status, Running Time, and CPU Usage. The table lists eight virtual machines: Alpha, Bravo, Oscar, Papa, Quebec, Romeo, Sierra, and Tango, all currently off. The CPU usage for all is listed as "n/a".

| Virtual Machine Name | Status | Running Time | CPU Usage |
|----------------------|--------|--------------|-----------|
| Alpha | Off | n/a | n/a |
| Bravo | Off | n/a | n/a |
| Oscar | Off | n/a | n/a |
| Papa | Off | n/a | n/a |
| Quebec | Off | n/a | n/a |
| Romeo | Off | n/a | n/a |
| Sierra | Off | n/a | n/a |
| Tango | Off | n/a | n/a |

Hyper-V

Unlike Virtual Server 2005 R2's application-based architecture, Windows Server 2008's Hyper-V is a core function built in to the actual operating system.

The most significant improvements of Hyper-V over Microsoft's previously offered virtualization technology, Virtual Server 2005 R2, are listed in Table 8.1.

Table 8.1 Feature Comparison between Windows Server Hyper-V Virtual Server 2005 R2

| Feature Comparison | |
|---|--|
| Windows Server Hyper-V | Windows Virtual Server 2005 R2 SP1 |
| Support for 32-bit and 64-bit VMs simultaneously | Supports only 32-bit guest VMs |
| Up to 32Gb of memory and 8 CPUs for each VM | Up to 3.6Gb of RAM and 1 CPU per Guest VM |
| Support for quick migration | Not supported |
| Support for network load balancing between VMs | Not supported |
| Support for virtual VLANs | Not supported |
| SCVMM 2007 not supported A promised upgrade in the next pending release of SCVMM 2007, due out in mid-2008. | Integration with SCVMM 2007 Current release of SCVMM 2007 only supports Virtual Server 2005 R2-based virtual assets. |
| Support for Virtual Machine Snapshots | Virtual Server 2005 R2 also supports this functionality |

Configuration

Once all previously discussed hardware specific prerequisites involving supported processor, updated BIOS, and enabled BIOS settings have been met, it is necessary to download and install the Hyper-V RCO update. This update must be installed first; otherwise, the Virtualization Role will not be available for selection and installation under Server Manager.

The required version of the update to be applied depends upon whether you are running a 32-bit or 64-bit host. Under the current RTM release of Windows Server 2008 they are as follows:

- Update for Windows Server 2008 KB949219
- Update for Windows Server 2008 x64 Edition KB949219



TEST DAY TIP

It is important to note that the above-mentioned update may change after the final release of Hyper-V, due out in mid-2008.

Once the prerequisite update has been installed you can proceed to the installation of the Windows Server Virtualization Role.

Installing the Virtualization Role on Windows Server 2008

The Windows Server Virtualization (WSv) Role can be installed by one of two methods:

- **From the command line** On a Windows Server 2008 Core Server Installation, the Windows Server Virtualization Role can be installed by running the command **Start /w ocsetup Microsoft-Hyper-V**.
- **From Server Manager** The WSv Role can be installed from Server Manager, but only on a full installation of Windows Server 2008 Full. Perform the following to accomplish this task: Select **Start | All Programs | Administrative Tools | Server Manager**, then select Roles, and then from the right-hand pane select Add Roles.



TEST DAY TIP

It is important to note that once the Hyper-V Role has been successfully installed on a Server Core instance of Windows Server 2008 it is necessary to connect to a new instance from another server running either a full install of Windows Server 2008 or a Windows Vista computer running the appropriate tools. This is because a Server Core installation does not have the Server Manager GUI tool available for WSv Role management.

It is also important to remember that Server Roles cannot be installed through Server Manager while connected remotely to another Windows Server 2008 instance. Roles can only be installed while connected locally.

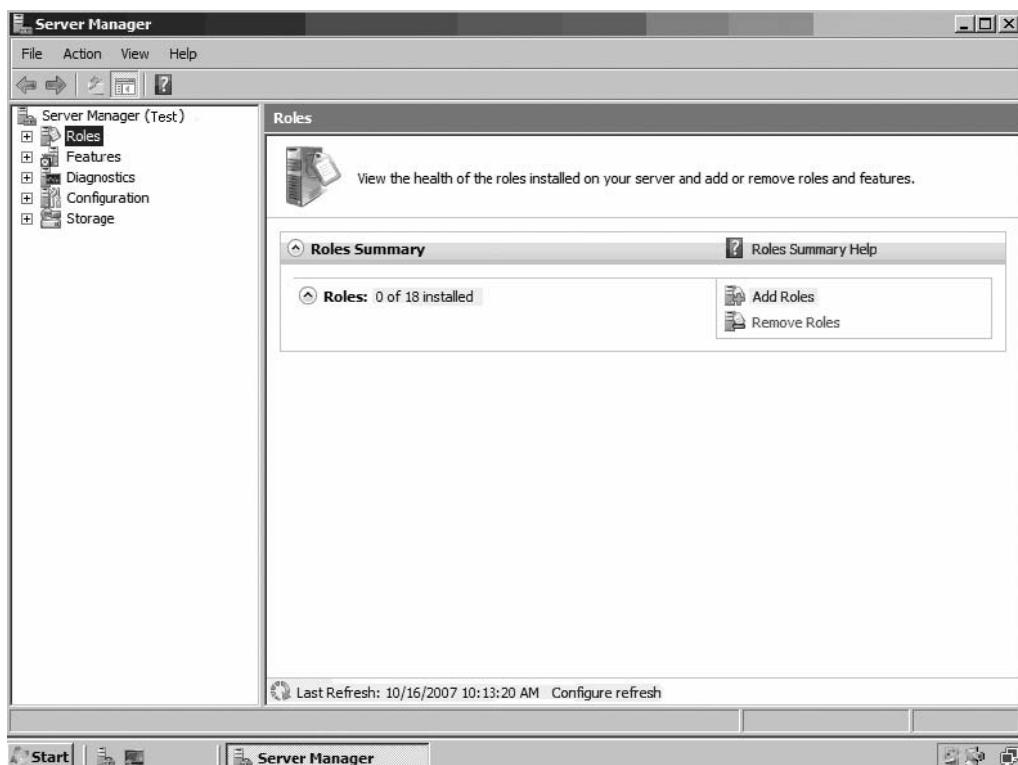
EXERCISE 8.1

INSTALLING THE VIRTUALIZATION ROLE ON A FULL INSTALLATION OF WINDOWS SERVER 2008

As a prerequisite, this exercise assumes the pre-existence of a full installation of Windows Server 2008 that has been fully configured with all supporting requirements in place. This includes the enabling of the required BIOS settings needed to support Windows Server Virtualization.

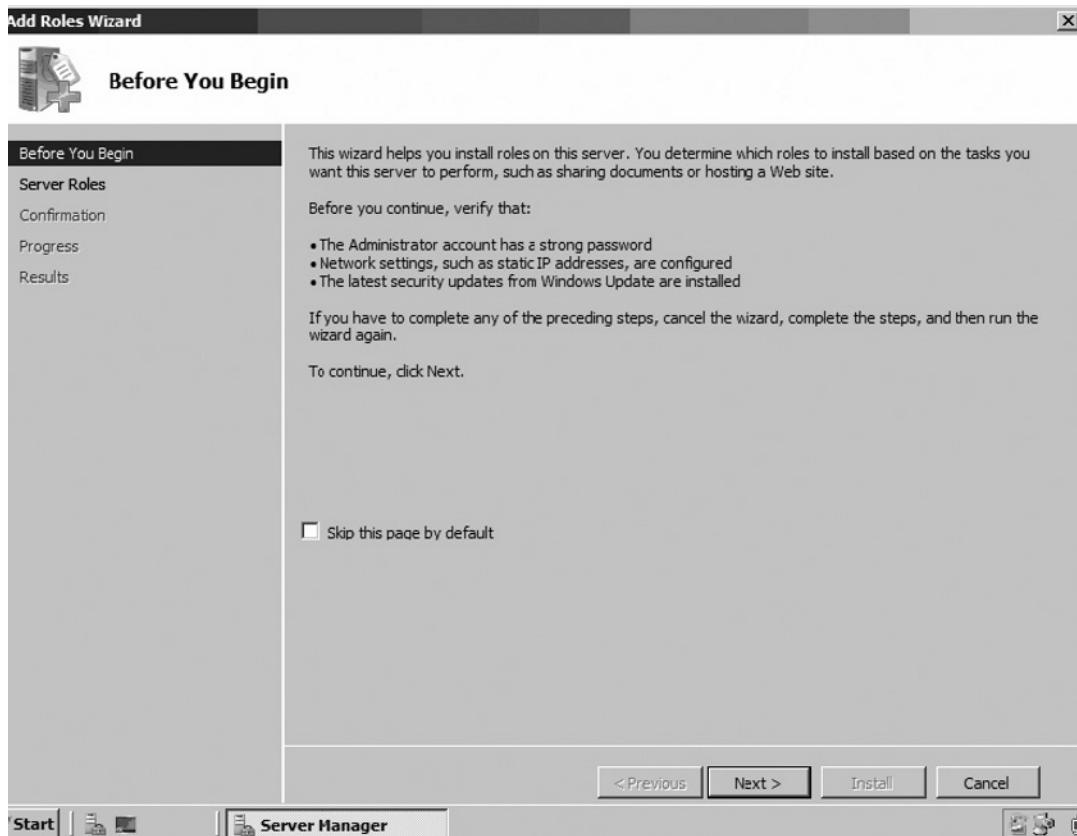
1. Log on to the Windows Server 2008 instance using an account possessing administrative privileges.
2. Install the **Update for Windows Server 2008 KB949219** (either 32 or 64 bit).
3. Reboot the server when prompted.
4. Select **Start | Administrative Tools | Server Manager | Roles**.
5. Select the **Add Roles** link (see Figure 8.5).

Figure 8.5 Server Manager “Add Roles” Page

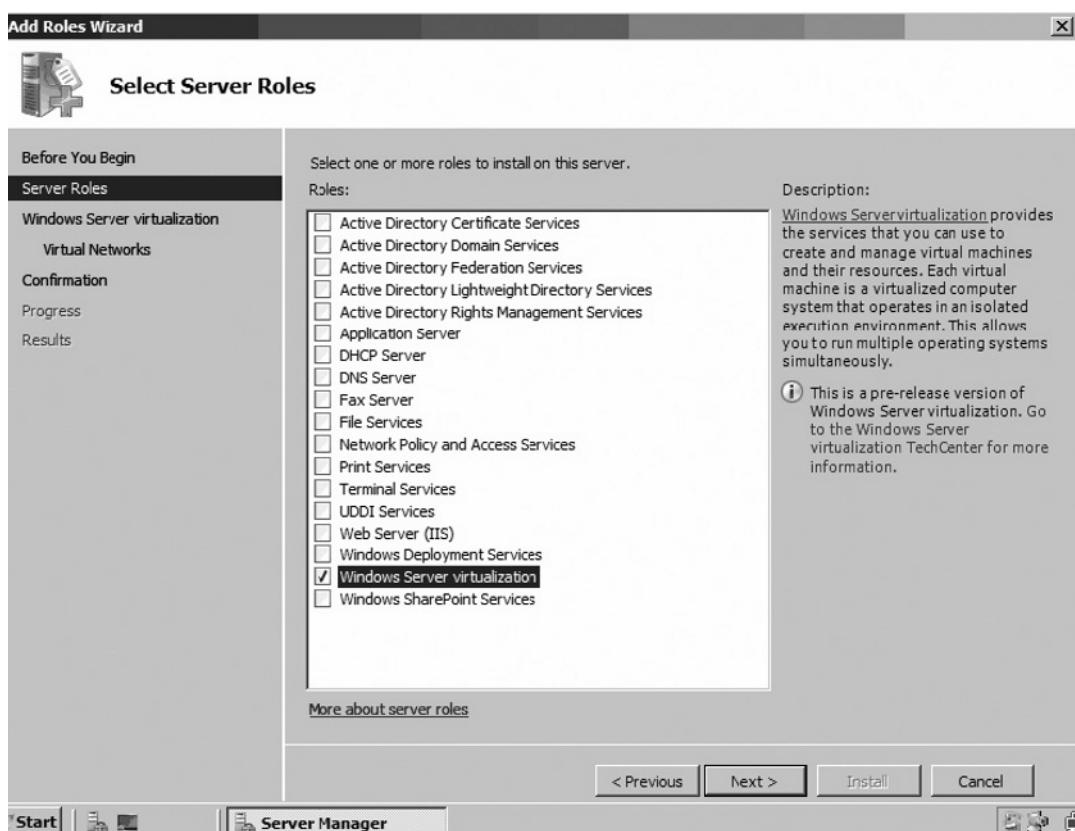


6. On the **Before You Begin** page, ensure prerequisites are met; then click **Next** (see Figure 8.6).

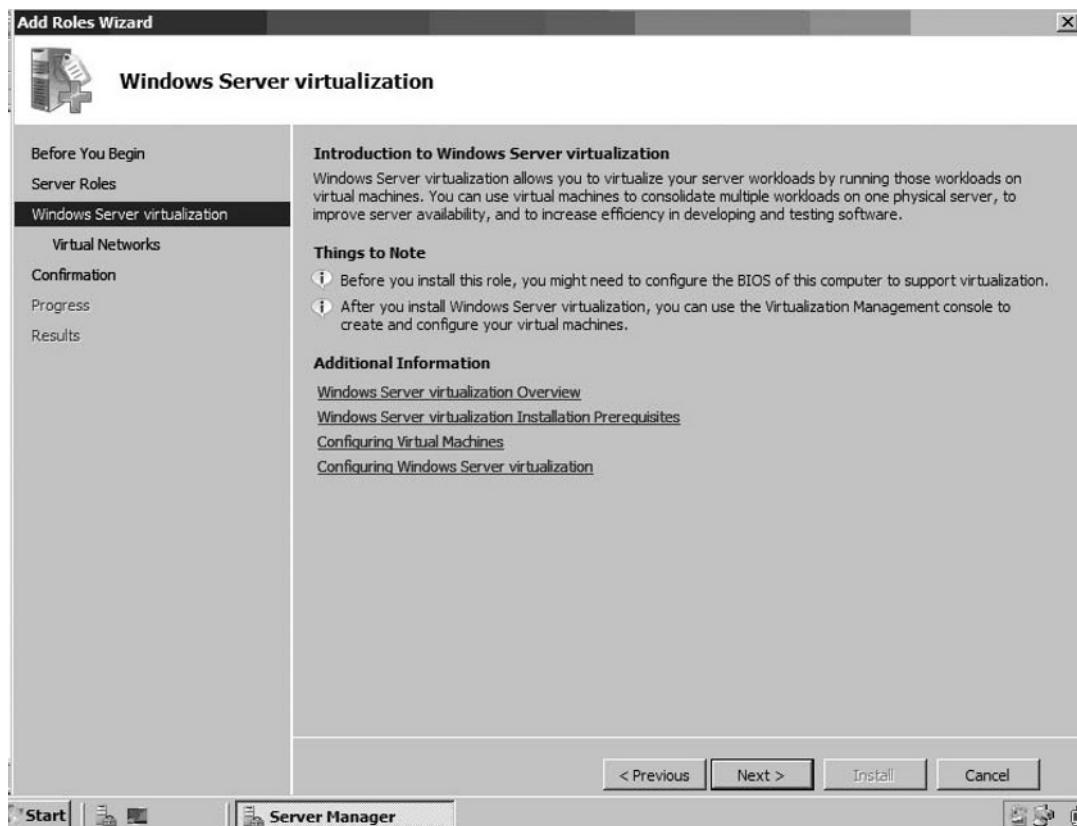
Figure 8.6 Add Roles Wizard Before You Begin Page



7. On the **Select Server Roles** page, select the role called **Windows Server Virtualization**, then click **Next** (see Figure 8.7).

Figure 8.7 Add Roles Wizard Select Server Roles Page

8. Next, you will be presented with the **Introduction to Windows Server Virtualization** screen. Read the **Things to Note** section to ensure compliance. Click **Next** (see Figure 8.8).

Figure 8.8 Add Roles Wizard Windows Server Virtualization Page

9. The next screen to appear, **Add Roles Wizard Create Virtual Networks**, allows for the creation of virtual networks (see Figure 8.9).
10. Once complete, click **Next** to continue.

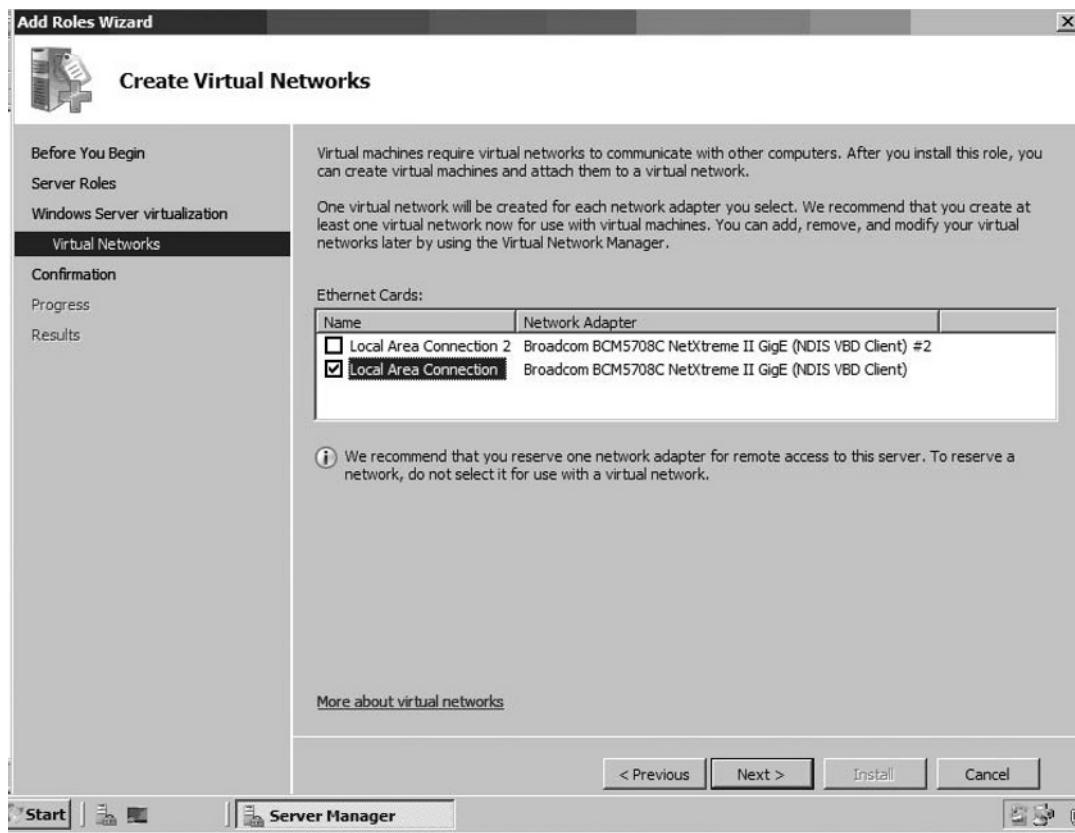
NOTE

The network adapter selected here will be used to create a virtual network for virtual machines running on this host. This virtual network will be used for all network communications between virtual machines within the virtual environment of this host, as well as to outside network. It is recommended that one adapter be reserved for remote console connectivity to the host computer.

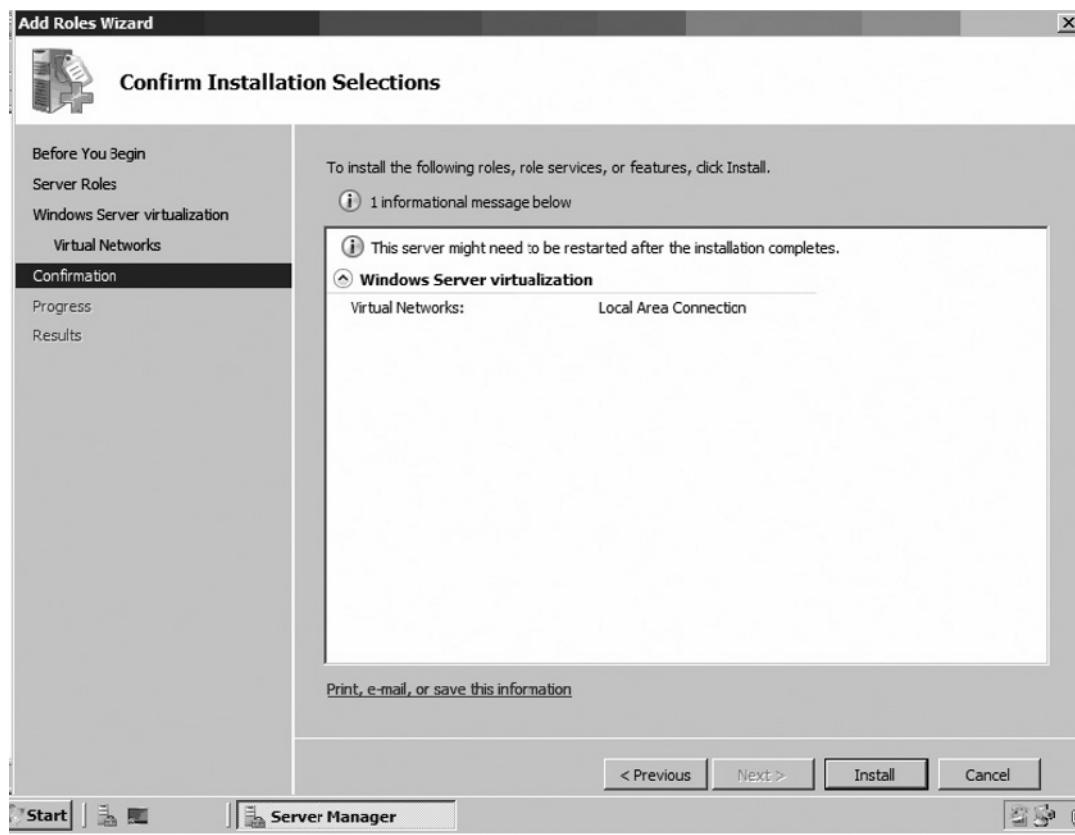
TEST DAY TIP

To reserve an adapter for console communication just don't select it this page.

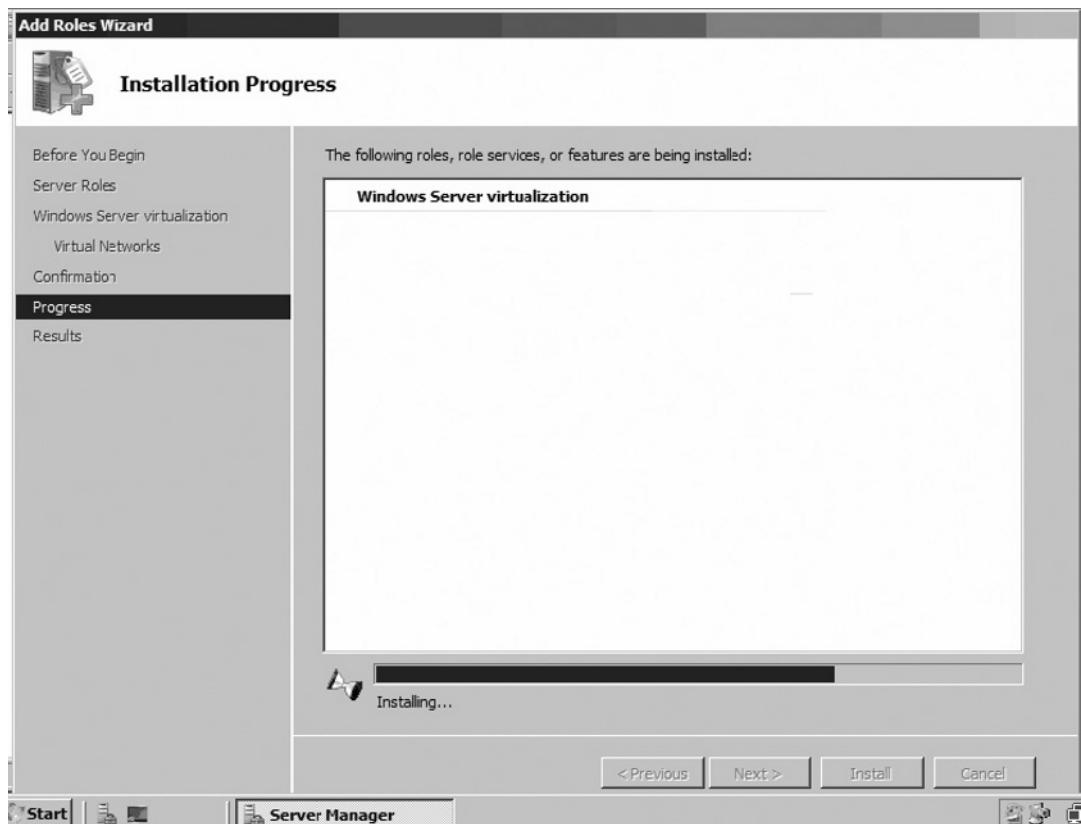
Figure 8.9 Add Roles Wizard Create Virtual Networks Page



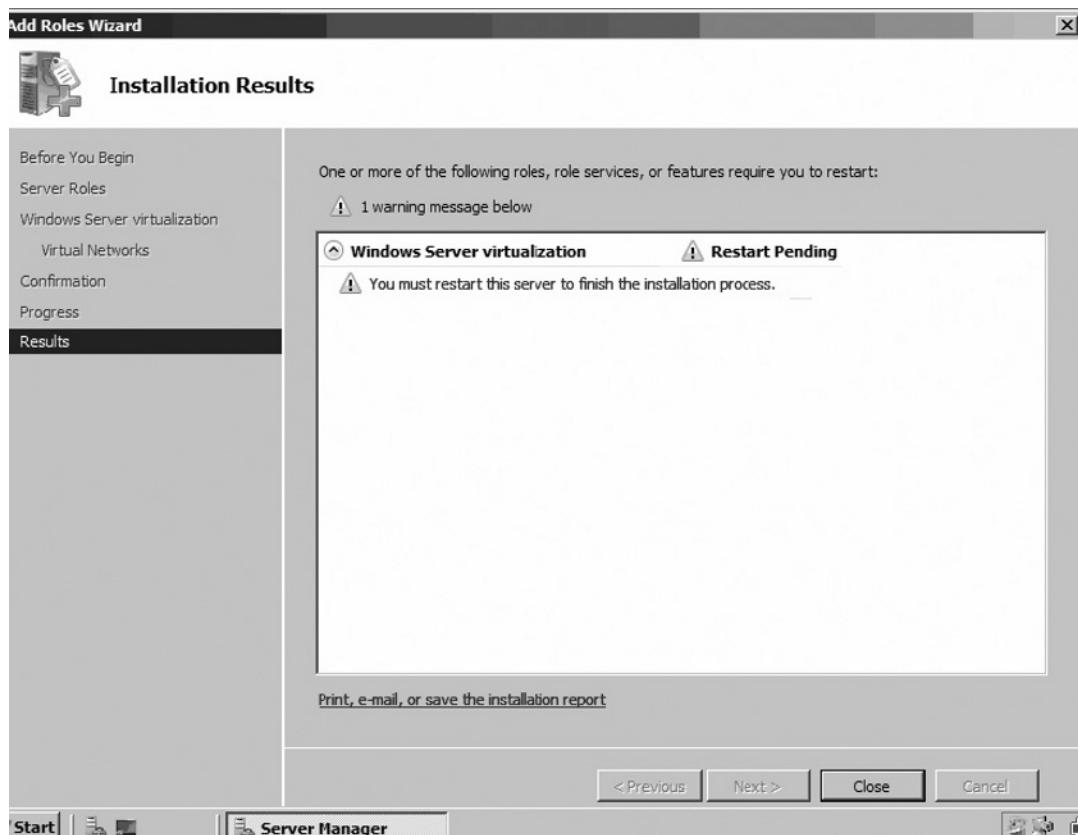
11. The **Confirm Installation Selections** screen, shown in Figure 8.10, displays the results of previous choices. The information most important to confirm is the choice of network adapter. When satisfied with the choices displayed click **Next** to continue.

Figure 8.10 Add Roles Wizard Confirm Installation Selections Page

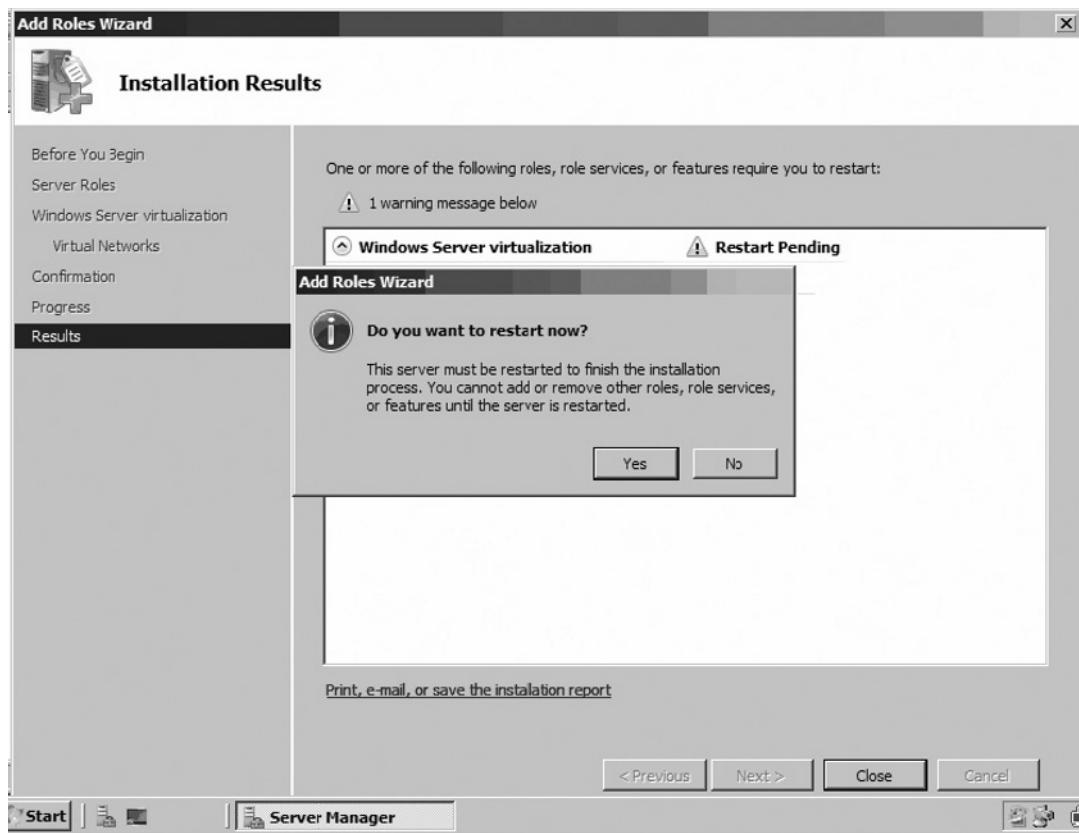
13. The **Installation Progress** screen will then appear showing that the actual installation phase has started (see Figure 8.11).

Figure 8.11 Add Roles Wizard Installation Progress Page

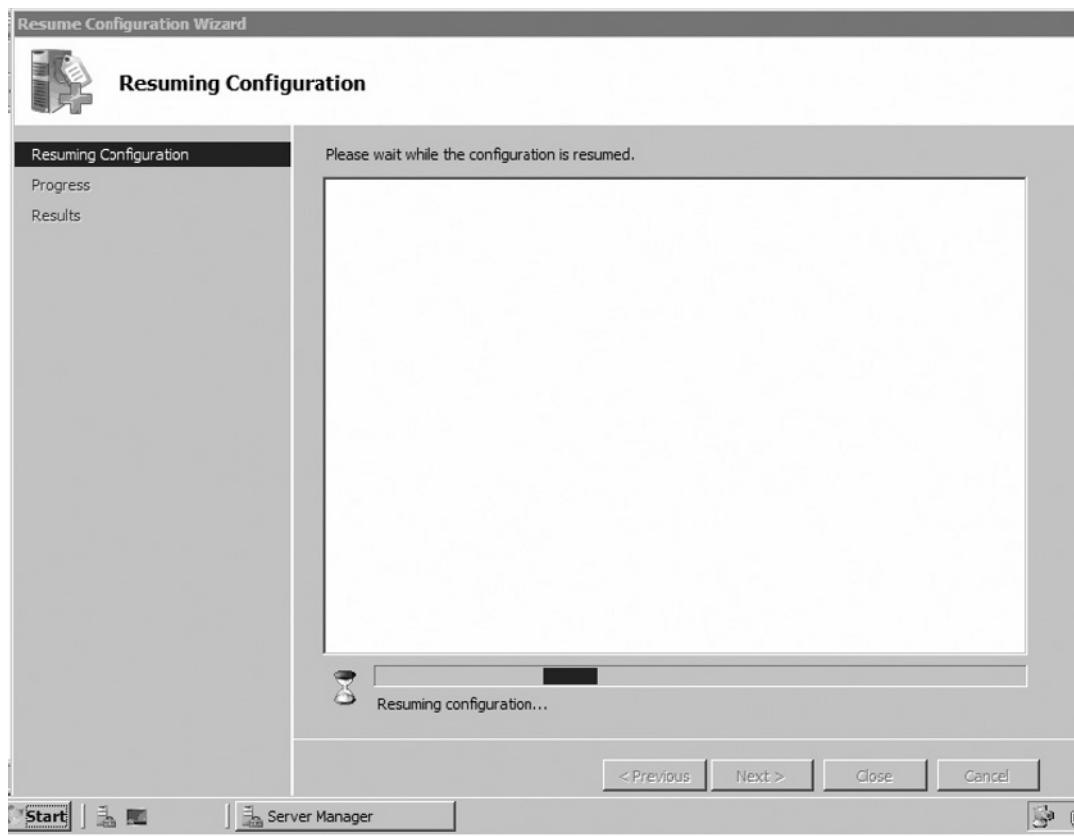
14. Once the **Installation Result** page appears, you will see the notice that a restart is pending. Select **Close** at the bottom to continue with the installation (see Figure 8.12).

Figure 8.12 Add Roles Wizard Installation Results Page

15. Once the **Installation Results** page appears you will see the notice that a restart is pending. Select **Close** at the bottom to continue with the installation (see Figure 8.13).

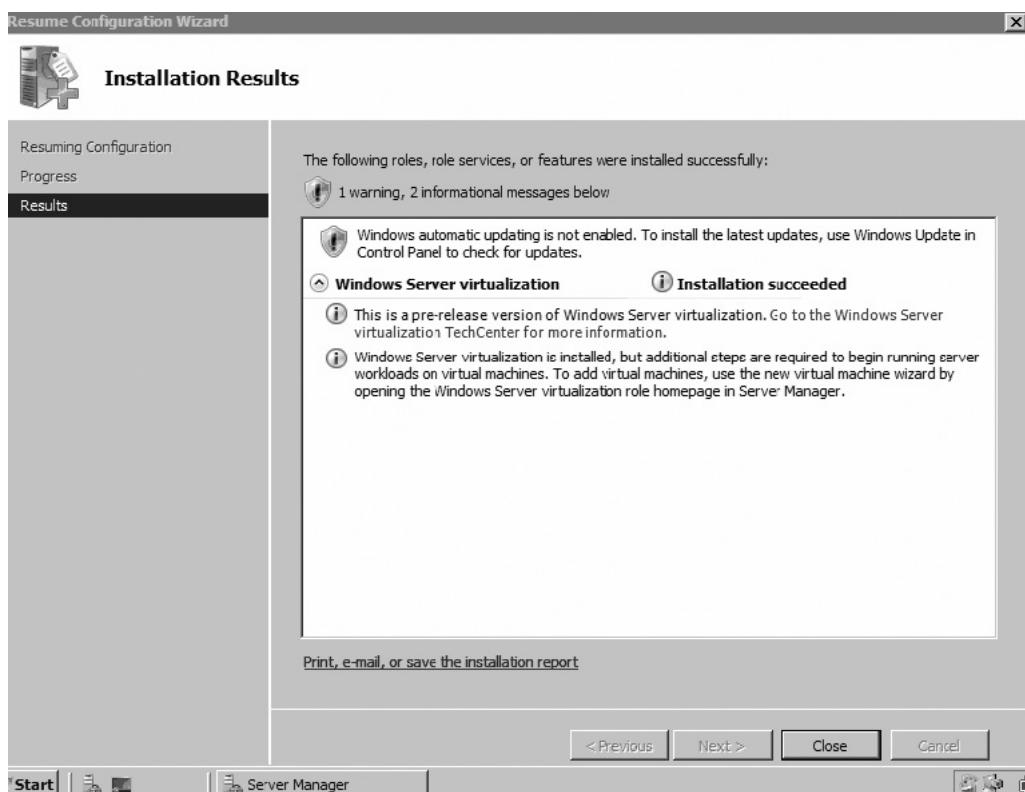
Figure 8.13 Add Roles Wizard Installation Results

16. After the reboot, log on again. The installation will resume, as shown in Figure 8.14.

Figure 8.14 Add Roles Wizard Resuming Configuration Page

17. Select **Close** to close the wizard and complete the addition of the Windows Server Virtualization Role (see Figure 8.15).

Figure 8.15 Add Roles Wizard Installation Results Page



The Windows Server Virtualization Role has now been successfully installed on your computer and you can log on again.

After the installation of the Windows Server Virtualization Role, the Windows Virtualization Manager snap-in will now be available from either one of two locations (see Figure 8.16):

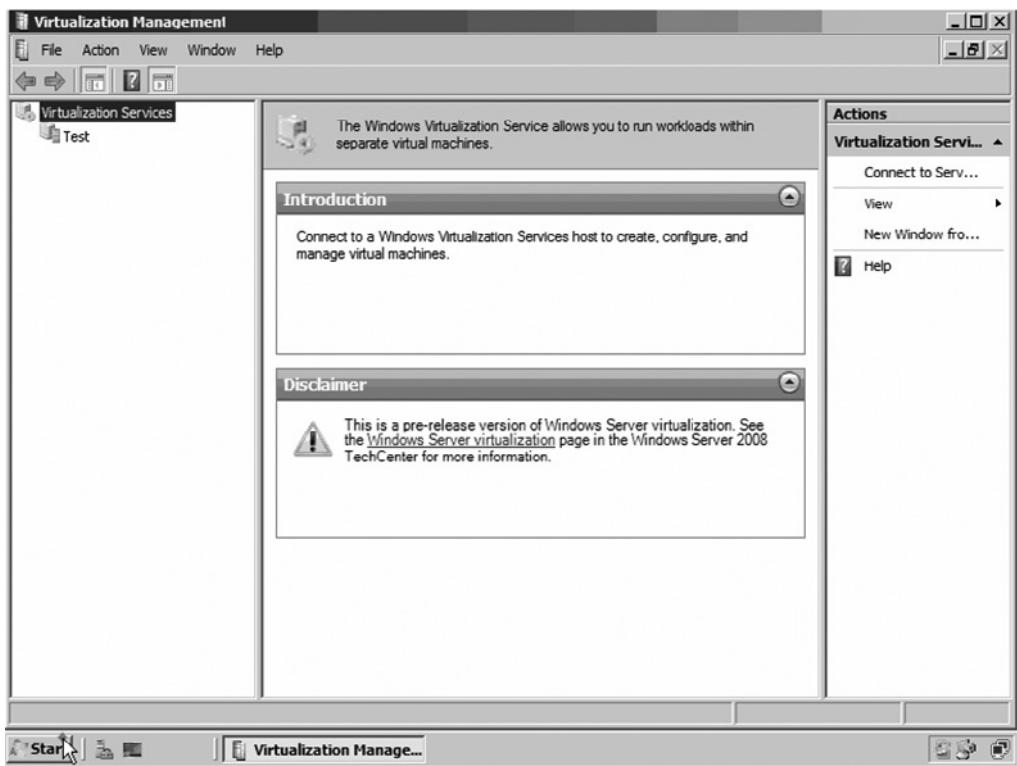
- **Server Manager | Roles | Windows Server Virtualization** snap-in
- Stand-alone **Windows Server Virtualization Manager**, available under Administrative Tools

The two management consoles are essentially identical from the perspective of managing virtual assets. The only real difference is that Server Manager contains other functionalities and tools for management of server properties not related to virtualization. For that reason, the most likely choice for the management of virtual assets is the Stand-Alone Windows Server Virtualization Manager MMC.

NOTE

When Hyper-V Manager is opened for the first time, the EULA must be accepted while logged on with an account possessing Local Admin privileges; otherwise, the console will not function properly.

Figure 8.16 Stand-Alone Windows Server Virtualization Snap-In



Configuring Virtual Servers with Hyper-V

VMs can be created using one of three management tools in Windows Server Virtualization:

- Server Manager | Roles | Virtual Machine Manager Console
- Stand-alone Virtual Machine Manager Console
- System Center Virtual Machine Manager 2007 Console

Any one of these three interfaces will allow you to accomplish the same tasks. Despite some functionality differences, each of these management tools is laid out in the same common format: Hierarchy in the left-hand pane, Content in the middle pane, and Tasks and tools in the right-hand pane.

Therefore, in all three cases the tools required to create new virtual machines will be found to the right side of the snap-in. The structure under which the newly created virtual machines will be organized will be found to the left of the console, and the newly created virtual machines themselves will be displayed in the center portion of the console.

Methods available to create a new virtual machine with Windows Server Virtualization are as follows:

- A physical to virtual computer conversion (P2V)
- A virtual to virtual machine (V2V) conversion
- Migrate an existing virtual machine with the .vhdx format
- Create from an already existing virtual hard disk
- Create from a previously configured virtual template
- Create a new blank virtual machine and install an O/S manually

Newly created virtual machines can be configured as per the following constraints. For the guest operating system, the following are the available supported options:

- Windows Server 2008 (all 32-bit and 64-bit versions)
- Windows Server 2003 (all 32-bit and 64-bit versions)
- Windows Vista SP1 and Windows XP SP3
- SuSE Linux Enterprise Server 10 SP1 (beta x86 and x64 editions)

NOTE

At the time of writing, Windows Server 2008's Hyper-V is at Release Candidate 0. These options may change in the final release version, due out in mid-2008.

For the assignable system resources, the following are the available options:

- Up to 64Gb memory per VM
- Up to 4 virtual SCSI disks per VM
- Up to 4 processors per VM with the Windows Server 2008 guest o/s
 - Maximum of 2 processors per Windows Server 2003 32-bit guest o/s.
 - Maximum of 1 processor per Windows Server 2003 64-bit guest o/s.
- Up to 8 virtual network adapters per VM.

EXERCISE 8.2

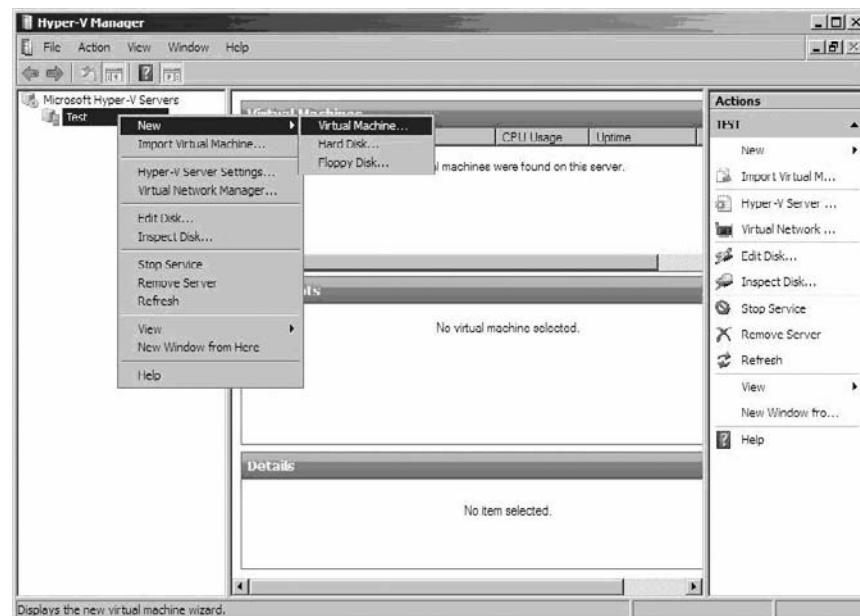
CREATING A VIRTUAL MACHINE USING WINDOWS SERVER 2008's STAND-ALONE HYPER-V MANAGER CONSOLE

1. Log on to Windows Server 2008 using an account with administrative privileges.
2. Select **Start | Administrative Tools | Windows Server Virtualization.**

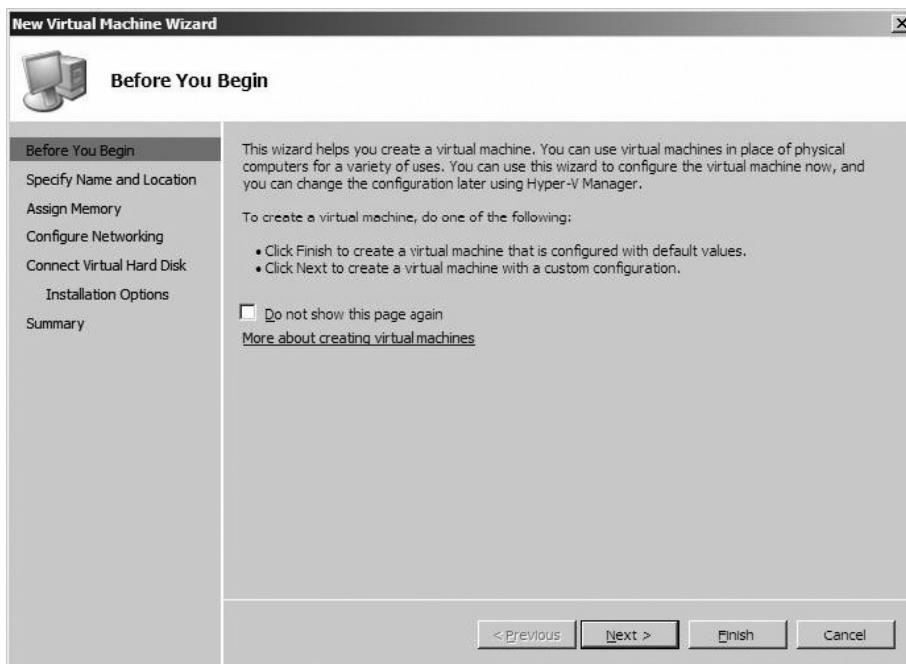
NOTE

When Hyper-V Manager is opened for the first time, the EULA must be accepted while logged on with an account possessing Local Admin privileges; otherwise, the console will not function properly.

3. Right click in the left pane and select **New** and then select **Virtual Machine** (see Figure 8.17).

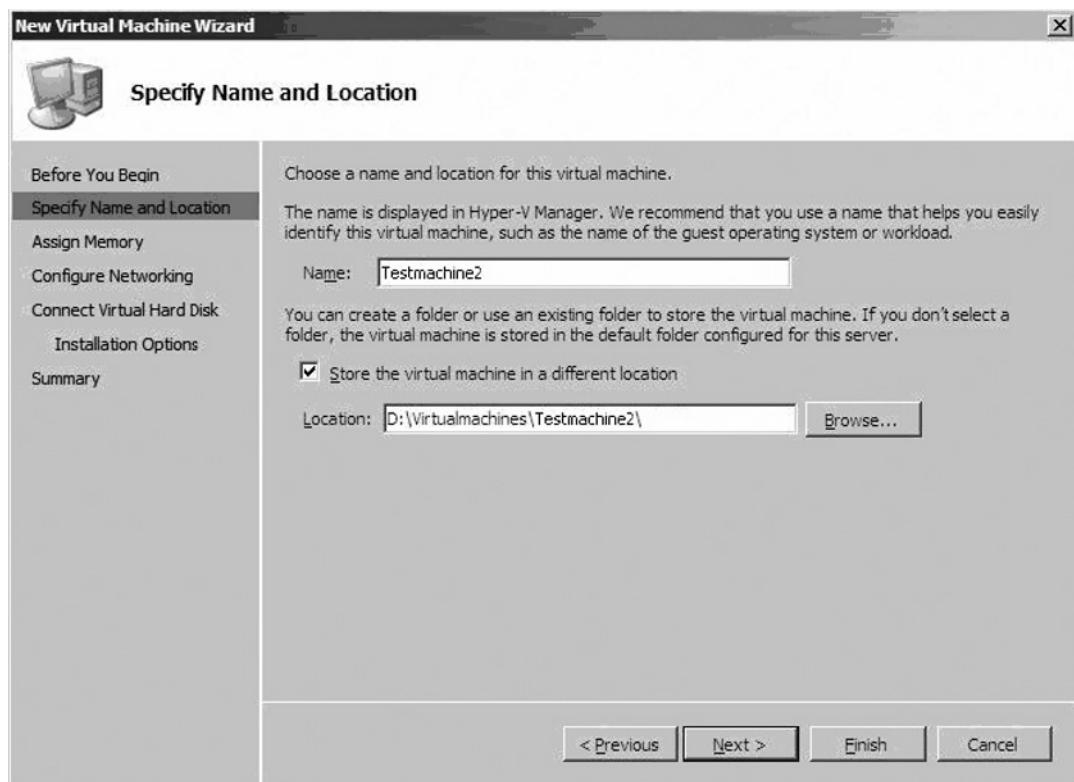
Figure 8.17 The Hyper-V Manager Console

4. The **Before You Begin** page is informational. Select **Next** to proceed (see Figure 8.18).

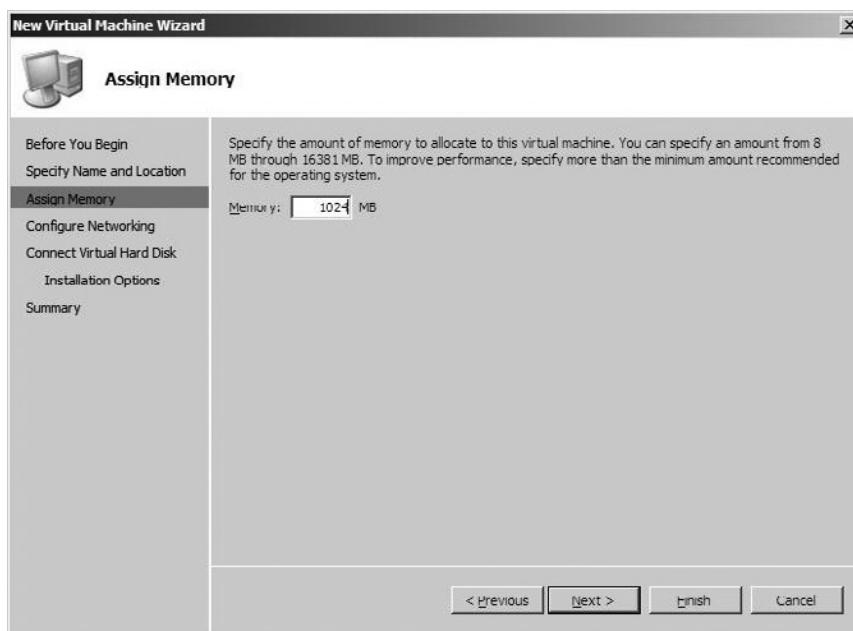
Figure 8.18 New Virtual Machine Wizard Before You Begin Page

5. The **Specify Name and Location** page provides the name of the virtual machine being created. Check the **Store the Virtual Machine in a different location** check box, and then provide the path to your chosen location. Click **Next** (see Figure 8.19).

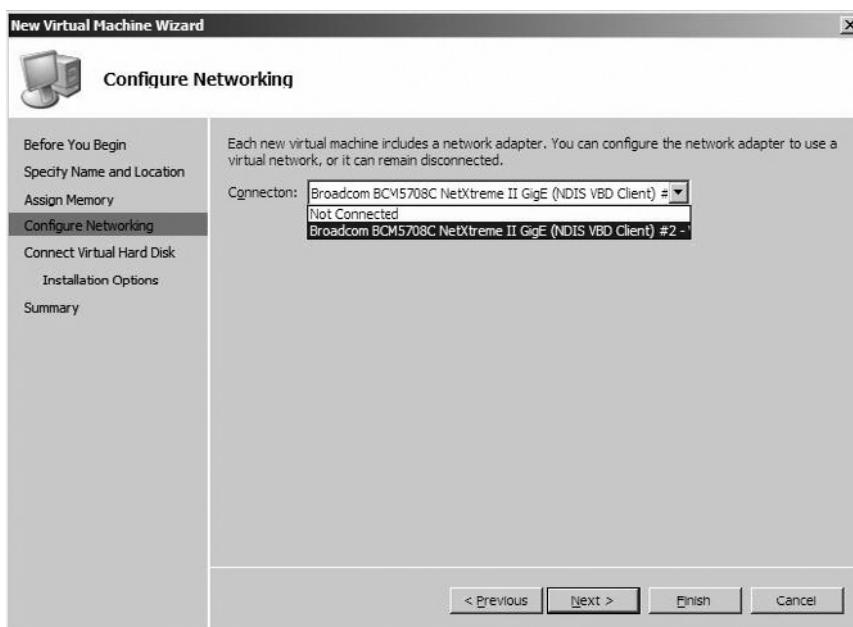
Figure 8.19 New Virtual Machine Wizard Specify Name and Location Page



6. In the **Assign Memory** page, allocate the VM's memory and then select **Next** (see Figure 8.20).

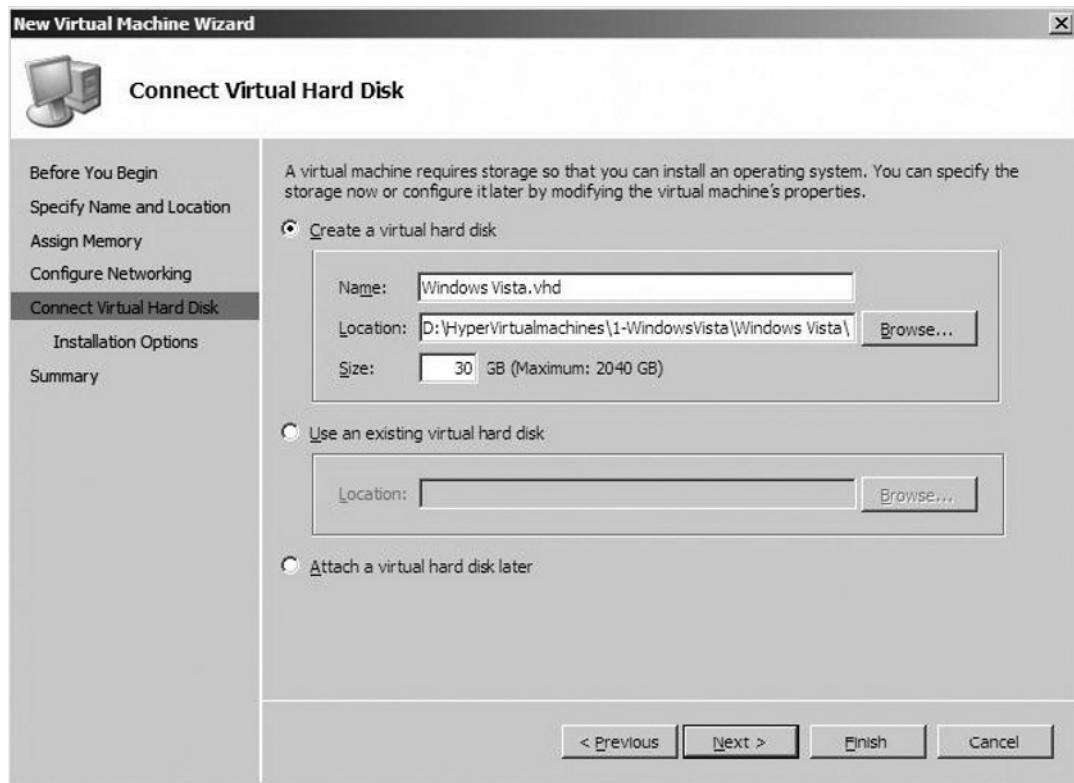
Figure 8.20 New Virtual Machine Wizard Assign Memory Page

7. In the **Configure Networking** page, choose the network adapter that you want the virtual machine to use for network communication (see Figure 8.21).

Figure 8.21 New Virtual Machine Wizard Configure Networking Page

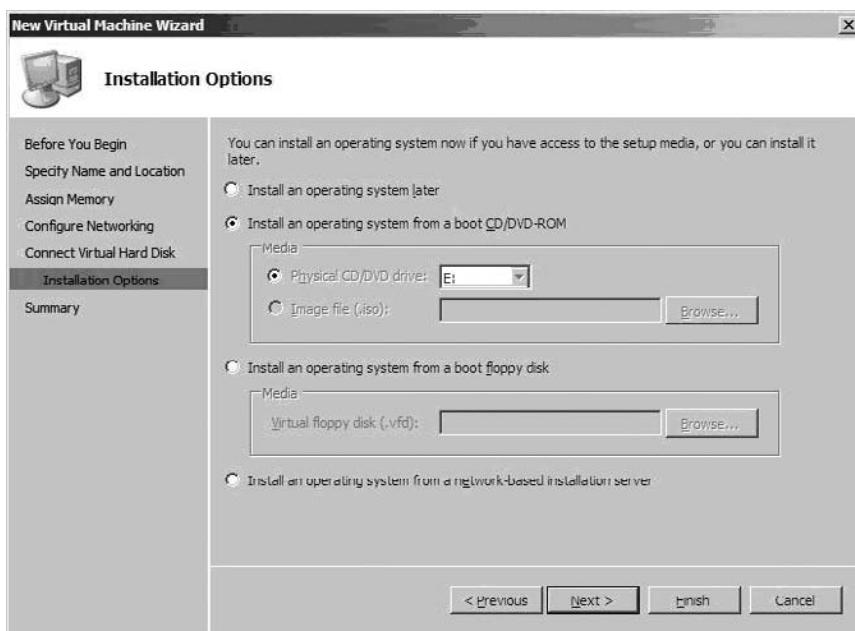
8. In the **Connect Virtual Hard Disk** page, provide the file name, storage location, and size of the .vhd virtual disk file to be attached to the new VM then select **Next** (see Figure 8.22).

Figure 8.22 New Virtual Machine Wizard Connect Virtual Hard Disk Page



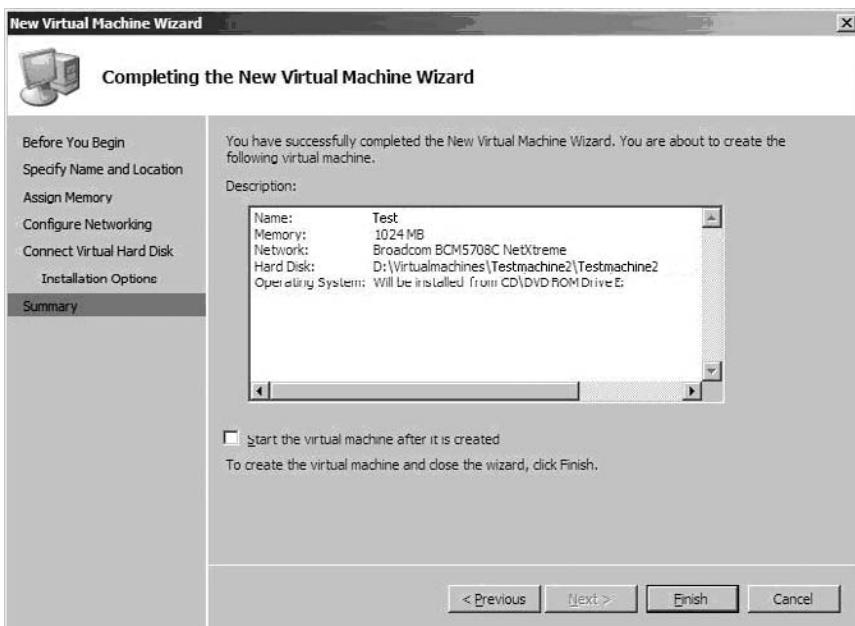
9. In the **Installation Options** page, provide four options for the installation of an O/S. Choose **Install from a boot CD/DVD-ROM**. Select **Next** to proceed (see Figure 8.23).

Figure 8.23 New Virtual Machine Wizard Installation Options Page



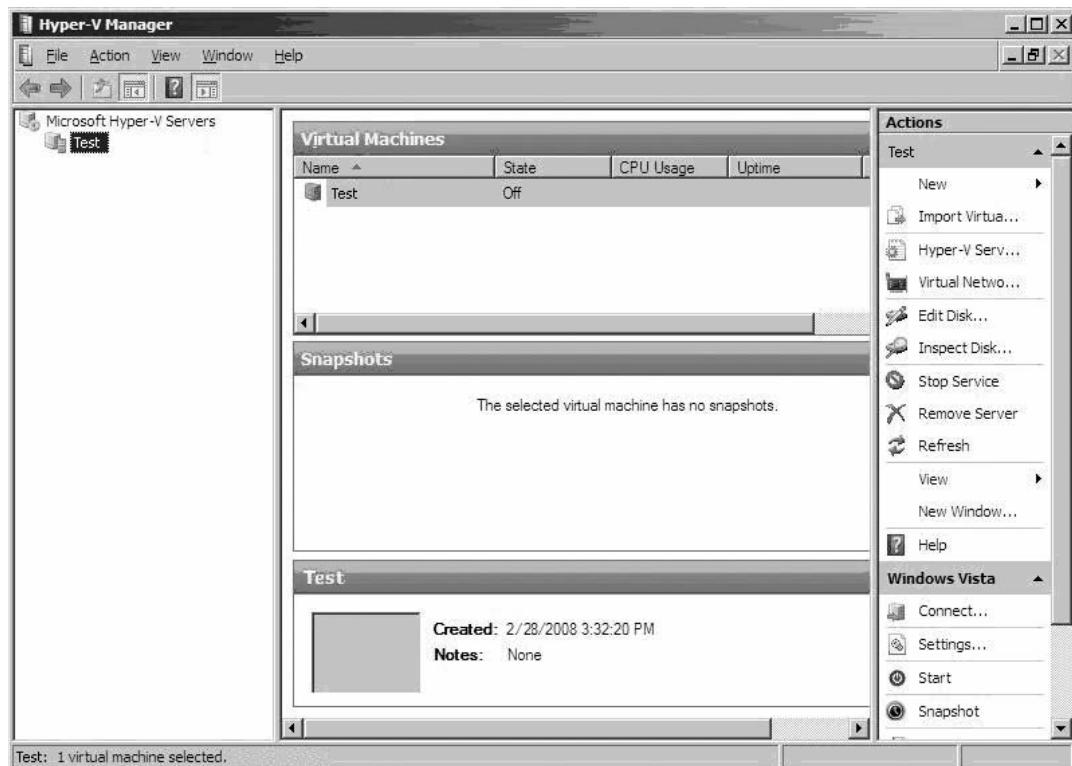
10. After reviewing all selections select, select **Finish** to create the virtual machine (see Figure 8.24).

Figure 8.24 New Virtual Machine Wizard Completing the Wizard Page

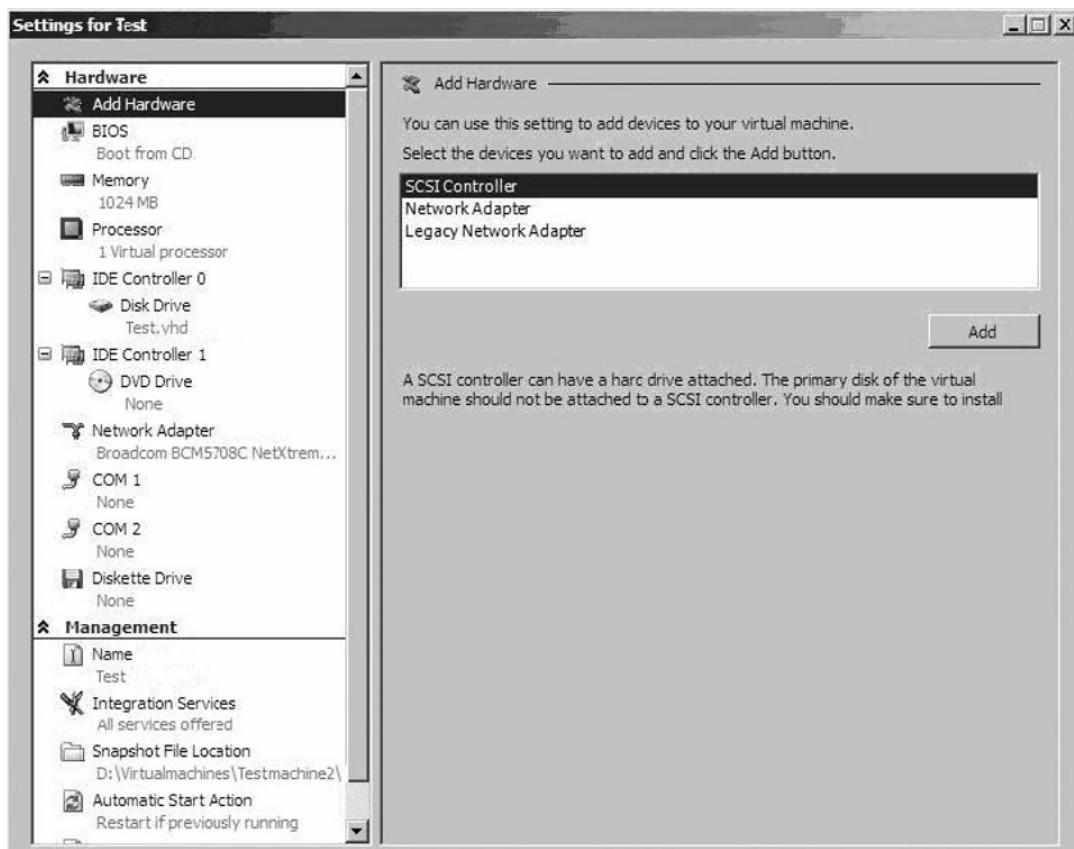


11. Once completed, reopen **Hyper-V Manager** to view the newly created virtual machine (see Figure 8.25).

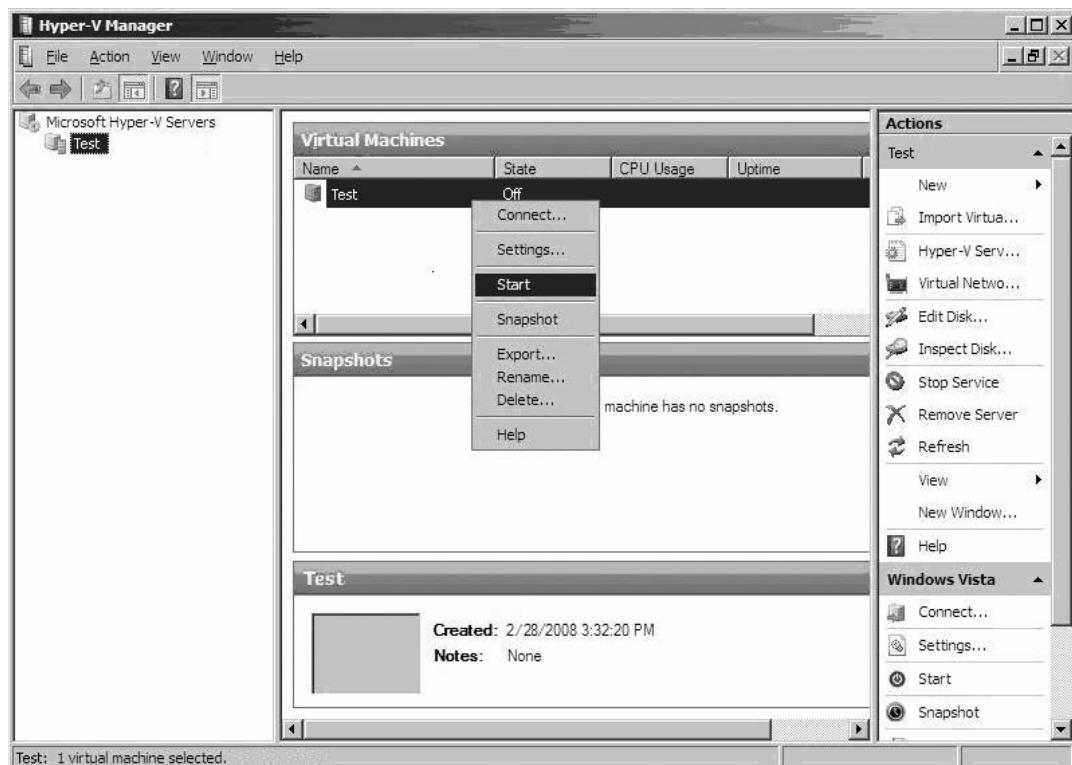
Figure 8.25 The Hyper-V Manager Console



12. Right click on the new virtual machine and select **Settings** to view available options (see Figure 8.26).

Figure 8.26 Settings for Virtual Machine Page

13. After reviewing the available options, select **Close** to close the settings page.
14. Place a CD containing the desired operating system media into the physical CD drive on the host computer.
15. Right click on the virtual machine under Hyper-V Manager and select **Start** (see Figure 8.27).
16. Right click again on the virtual machine and select **Connect** to initiate a remote control session.
17. Once the virtual machine has successfully booted to your media, proceed with operating system installation to complete the virtual machine creation process.

Figure 8.27 The Hyper-V Manager Console Start Virtual Machine Page

You have now successfully completed the create virtual machine process using the stand-alone Hyper-V Manager Console.

Server Core

Windows Server 2008 Server Core installation is the recommended platform on which to deploy the Hyper-V Virtualization platform. This is for two main reasons:

- **Security** A Server Core installation has fewer services running and fewer ports open, providing reduced opportunity for security related intrusions.
- **Resources** A Server Core installation has only the minimal functionality installed that is required for basic server functionality and, therefore, uses fewer resources while leaving more available for Windows Server Virtualization.

A Server Core installation does not provide the standard graphic user interfaces such as Server Manager that a full installation would normally provide.

Therefore, the options available for the management of a Server Core installation are as follows:

From the command-line interface:

- **Remote Management using terminal services**

Terminal Server Remote Admin Mode must be enabled on the Server Core installation by typing the following at the command prompt:

- **cscript scregedit.wsf /ar 0**

To allow pre-Windows Vista operating systems to connect to your server via terminal services, it is necessary to disable enhanced security by typing the following at the command prompt:

- **cscript scregedit.wsf /cs 0**

Run **mstsc** from the remote computer and, when prompted, enter the name of the desired computer to which you wish to connect.

The available interface will be the command line with this method.

- **Remote Management using Server Manager** from another server running a full install of Windows Server 2008.

- **Remote Management using Remote Server Administration Tools** running on a Windows Vista workstation.



TEST DAY TIP

Server Roles cannot be installed through Server Manager while connected remotely to another Windows Server 2008 instance. Roles must be installed locally.

- **WMI Interface** from another computer using the appropriate tools

- **Windows Remote Shell** from another server running Windows Server 2008 or workstation running Windows Vista

This method can be used to run command line tools and scripts against a remote Server Core instance of Windows Server 2008.

Windows Remote Shell functionality must be enabled on the Server Core installation by typing the following at the command prompt:

- **WinRM quickconfig**

Launch from another computer by typing the following at the command prompt:

- **winrs -r:<servername><the desired command>**

NOTE

For a quick listing of a large number of general commands that can be executed at the command prompt of a Windows Server 2008, type the following at the command prompt:
cscript screredit.wsf /cli

Competition Comparison

Windows Server 2008 Virtualization introduces some important new feature and capabilities into the Virtualization market. Specifically, the introduction of hardware assisted virtualization represents a next generation type of advancement in the technology used to accomplish virtualization. Still, VMware's ESX Server is a mature product that has a significant head start in the industry.

Microsoft's Windows Server Virtualization is the first release from Microsoft to depart from the application layer approach to virtualization used by their previously available offering, Virtual Server 2005 R2. Microsoft has moved their technology forward with Hyper-V by taking the virtualization layer down to the operating system level in order to compete more seriously with the performance characteristics offered by VMware's ESX Server. While the operating system level virtualization layer has brought the performance of Windows Server Virtualization more in line with the competition, the first release of this product still has some catching up to do with the more mature feature set available to VMware's ESX customers.

One major advantage that the Microsoft product is providing over the VMware solution is that the Hyper-V add on Virtualization Server Role is being offered as a free add-on to any of the available versions of Windows Server 2008. This represents a huge cost advantage over the licensing model of the VMware solution. For large enterprise customers requiring the full feature set and time tested, proven industry track record offered by the ESX Server solution, it still appears VMware has a strong hold on the market over Microsoft's Windows Server Virtualization.

Another significant advantage that can be leveraged by Microsoft over the VMware solution is going to be in the availability of the accompanying resource

management package. The all-encompassing, heavily integrated enterprise resource management and monitoring solutions offered by Microsoft are all built on the same style of interface. Products such as System Center Virtual Machine Manager work seamlessly together with resource monitoring solutions such as System Center Operations Manager and others to cover all aspects of IT resource management requirements. This integration and cross compatibility makes for a much easier platform for IT administrators to learn and understand. Microsoft's common MMC design configuration with the hierarchy on the left, the content in the middle, and the tasks and tools on the right is a comfortable format to read and follow.

Other solutions utilizing multiple dissimilar tools, all with differing interfaces make for a more disjointed management experience that is generally more difficult to follow and track resources and their issues. This ultimately means that issues may not be noticed and addressed as efficiently and effectively. The one thing that VMware does not have at this point is the ability to offer a comparable, unified, and integrated multifaceted Management Solution for management and monitoring such as what Microsoft now has in place and available.

With respect to a feature-by-feature comparison of the two core virtualization engines that Windows Server is offering against the VMware ESX platform, there appear to be many direct similarities (see Table 8.2). The main difference where VMware's ESX pulls ahead is in the areas such as high availability and dynamic resource allocation (DRA). It is with these key mature features that the larger enterprise customers depend upon that ESX Server will maintain its market for the foreseeable future. Windows Server Virtualization will need to develop competitive feature offerings, if Microsoft wishes to compete seriously with VMware at the enterprise level.

Table 8.2 Feature Comparison between Windows Server Virtualization and ESX Server

| Feature Comparison | | |
|----------------------------------|-----------------------|-------------------------------|
| Feature | VMware ESX 3.X | Windows Server Hyper-V |
| Hypervisor | 32-bit monolithic | 64-bit microkernel |
| Hardware-assisted virtualization | No | Yes |
| 32-bit host support | Yes | No |
| 64-bit host support | Yes | Yes |

Continued

Table 8.2 Continued. Feature Comparison between Windows Server Virtualization and ESX Server

| Feature Comparison | | |
|----------------------------------|-----------------------|-------------------------------|
| Feature | VMware ESX 3.X | Windows Server Hyper-V |
| Maximum host CPUs | 32 | 32 |
| Maximum host memory | 128Gb | 1Tb |
| 32-bit VMs | Yes | Yes |
| 64-bit VMs | Yes | Yes |
| Maximum guest VMs | 128 | Unlimited |
| Guest SMPs | 4 | 8 |
| Maximum guest memory | 64Gb | 32Gb |
| Live VM migration (host to host) | Yes | No (supports quick migration) |
| Live VM Backup | Yes | No |
| Hot-add processors | No | Yes |
| Hot-add memory | No | Yes |
| Hot-add storage | No | Yes |
| Hot-add networking | Yes | Yes |

Server Placement

The proper placement of virtual servers within a virtual environment is dependant upon many factors. If multiple storage repositories such as multiple LUNs on a SAN are being utilized, then it is important to plan and place the virtual machines properly the first time. Moving the .vhd disk file to another storage location at a later time requires a shutdown of the virtual machine itself, and will result in an interruption of service to its end users.

The equal distribution of system resources such as processor power, and available memory is also an important consideration to be factored in. For a new virtual machine, performance history is obviously not available, but for a preexisting virtual machine that is being migrated into a virtual environment the existence of performance history can be invaluable in making the necessary decisions regarding where to place the virtual machine, and the level of system resources that should be allocated to it. Performance history can show information beyond what a given virtual machine is doing at any one given time. It can be used to determine periods of peak usage that may be consuming resources well above what the VM actually is consuming at the moment when its placement within an environment is being considered.

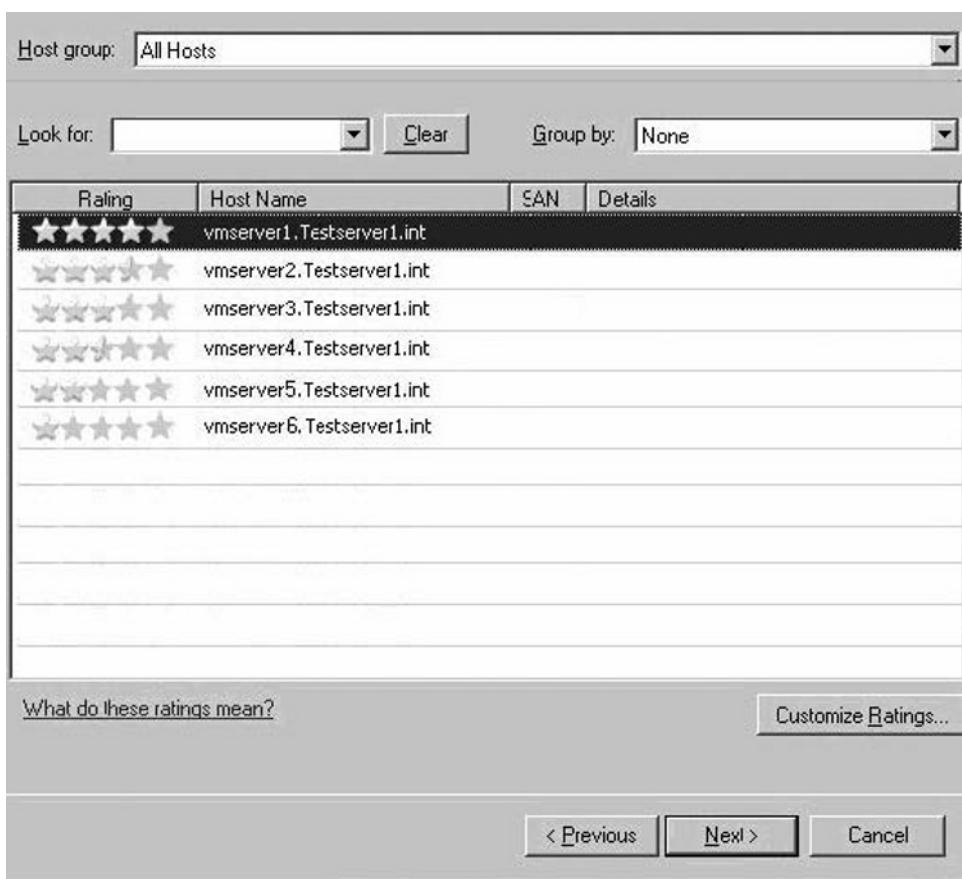
The virtual resource management tool discussed shortly provides a wizard-based capability that allows for a virtual machine's ideal placement to be considered and assessed based not only upon the anticipated resource utilization, but also on the intended goal of the administrator in choosing the placement. The system Center Virtual Machine Manager 2007 Console refers to this process as "Intelligent Placement," and contains a dedicated Intelligent Server Placement Tool, that offers two options for server placement criteria: load balancing algorithm and maximizing utilization algorithm.

This load balancing option would commonly be used in support of multiserver application farms, where servers are configured in an array-style format to accommodate the needs of end users on an "as resources are required" basis. Additional parameters can be adjusted within this tool to suit more specific requirements.

System Center Virtual Machine Manager (SCVMM) uses the following factors to make decisions and recommendations regarding ideal server placement (see Figure 8.28):

- Existing CPU, disk, RAM, and network resource utilization characteristics
- Historical CPU, disk, RAM, and network performance data, if available

Based upon the criteria listed above, an intelligent placement report is generated, ranking each available host according to its suitability for placement.

Figure 8.28 SCVMM Intelligent Placement Report

If System Center Operations Manager is also deployed in the environment for monitoring purposes, then this would be the location from where the needed performance data would be available. System Center Operations Manager can provide both the historical performance data required to make server placement decisions, as well as ongoing resource utilization monitoring. This ongoing monitoring capability can be used to monitor and optimize resource capacity moving forward.

System Center Virtual Machine Manager 2007

Virtual Machine Manager Server is a core application. It installs as a server-type application much like SQL Server 2005. It utilizes a SQL Server 2005 database

to store all virtual machine related metadata. It runs on either 32-bit or 64-bit version of Windows Server 2003.

System Center Virtual Machine Manager is optimized to manage Microsoft-based virtualization resources in a data center environment, although it does also possess the additional ability to convert VMware-based .vmdk format files into the .vhdx format utilized by Microsoft. This functionality is designed to allow for easy migration of virtual assets to the Windows Server Virtualization platform for those who wish to do so.

It is designed to work closely with and be utilized in conjunction with complimentary technologies such as System Center Operations Manager 2007, as well as other solutions designed to improve administrative efficiency and effectiveness in data center management.

The following versions of SQL Server 2005 are supported for the required database component of the installation: SQL Server 2005 Express and SQL Server 2005 Enterprise Edition.

The VMM Server can be accessed through any of the following interfaces:

- Virtual Machine Manager Administrator Console
- Self Service Web Portal
- Windows PowerShell command line utility

There are three main deployment scenarios for which the Virtual Machine Manager and its library infrastructure is designed to be configured:

- **Stand-Alone Instance** All required Virtual Machine Manager components, including the supporting virtualization platform and associated VMs, run on the same hardware
 - Virtual Server 2005 R2 or Windows Server Virtualization platform.
 - System Center Virtual Machine Manager 2007.
 - Local SQL Database.
 - Would most commonly be used for testing and development environments.
- **Corporate Data Center** Multiple System Center Application Servers designed to provide sufficient management capacity to handle the specific data center requirements
 - Separate Database and Library servers scoped to provide adequate capacity for the requirements of the host data Center.

- Servers can be configured for high availability solutions if required.
- Distributed DMZ-based clients are supported.
- **Enterprise Environment** Multiple System Center Servers at distributed locations to provide sufficient management capacity for distributed enterprise management requirements
 - Separate database and library servers scoped to provide adequate capacity.
 - Servers can be configured for high availability solutions if required.
 - DMZ-based clients are supported.

Virtual Machine Manager Administrator Console

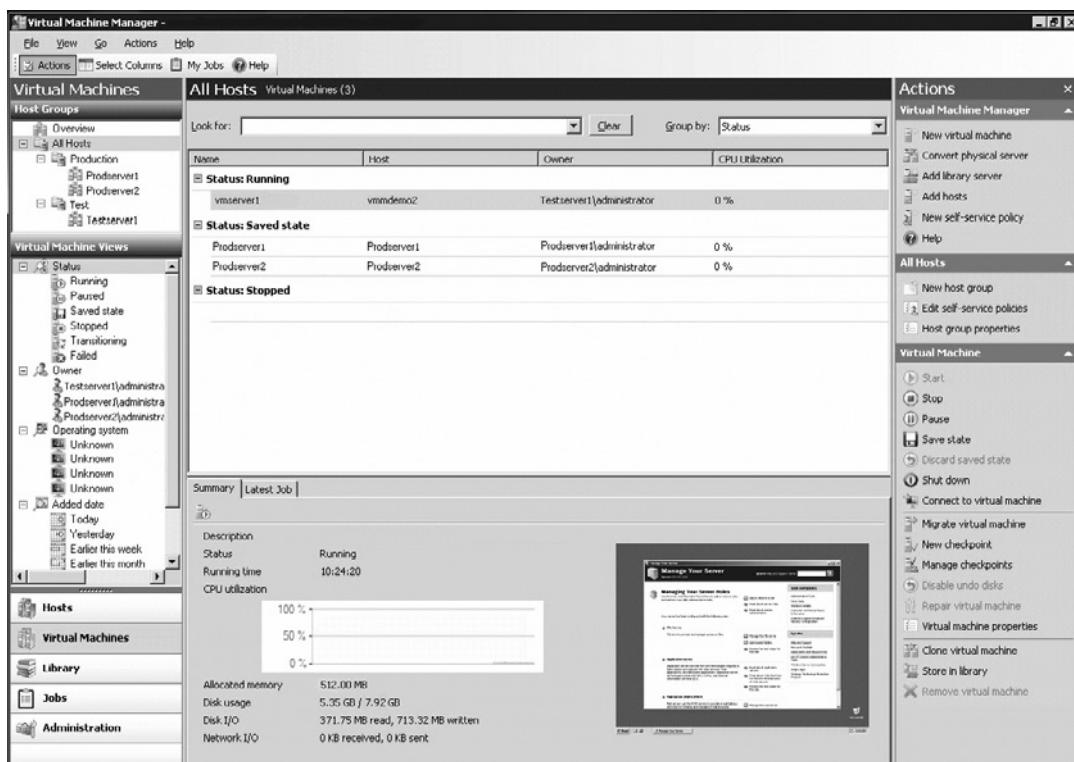
The System Center Virtual Machine Manager Administrator Console provides access to all the tools needed to perform virtual machine management for the following virtualized assets:

- Microsoft Virtual Server R2-based virtual assets
- Microsoft Windows Server 2008 virtual assets, which is promised in the next release

System Center Virtual Machine Manager Administrator Console integrates with System Center Operations Manager 2007 console to provide asset status and monitoring for virtual assets being managed under the SCVMM Console.

All tasks and tools available in the Administrative Console have a corresponding Windows PowerShell command, and all available wizards have the ability to display their associated commands (see Figure 8.29).

Figure 8.29 The Virtual Machine Manager Administrator Console



Designed according to the common Microsoft standard format of hierarchy on the left, content in the middle, and tools and tasks on the right, the System Center Virtual Machine Manager Administrative Console is straight forward and easy to use. In keeping with the Microsoft MMC format, the create New virtual machine Tool can be found as the first item on the list of available tools in the upper right corner of the Actions pane.

Unfortunately, at the time of this writing the available full release version of SCVMM only possesses the capability to manage Virtual Server 2005 R2-based virtual assets. At the time of the initial release of SCVMM 2007, Hyper-V was not yet available and, therefore, was not an included option. The next full release, due out in mid-2008, however, will contain the promised upgrades to include full Windows Server Virtualization technology management support.

Another common feature that has been repeatedly seen in the different Microsoft-based virtual machine management consoles is the thumbnail Console window in the lower right of the center Content section of the Management Console. The thumbnail window displays the remote console of the highlighted virtual server in the upper portion of the center Content section. The remote control console window can be quickly and easily opened by double clicking on the thumbnail image.

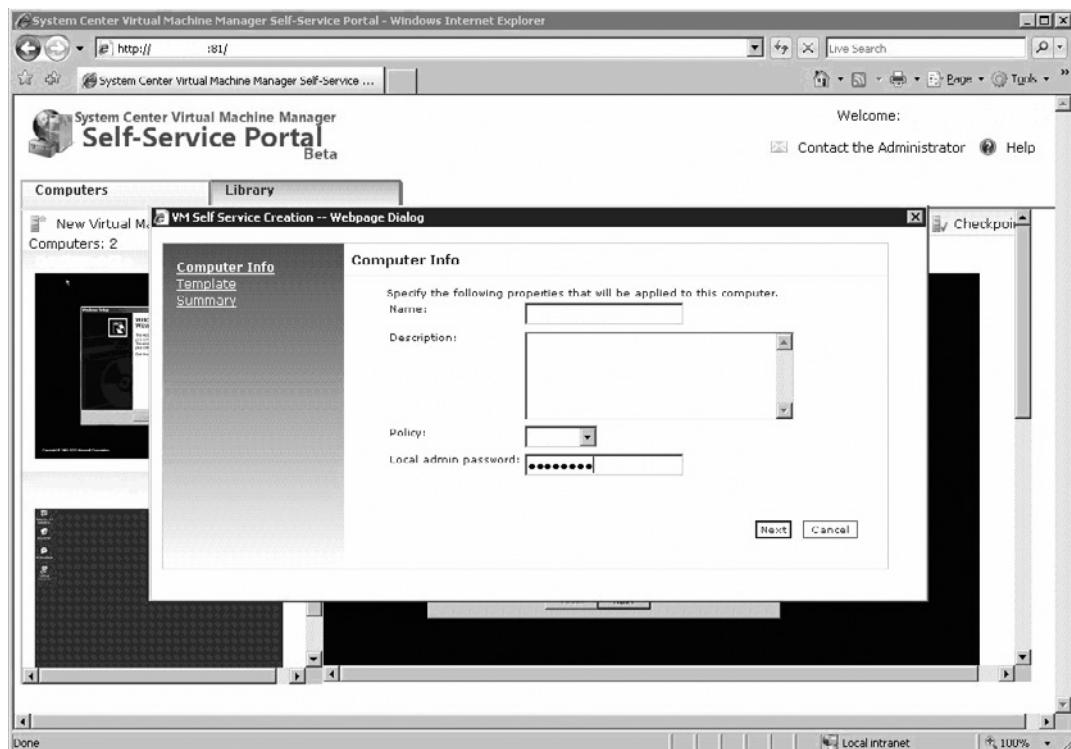
Windows PowerShell Command-Line Interface

Every Virtual Machine Manager task and tool has a corresponding Windows PowerShell command, which can be viewed during execution. This PowerShell capability can also be utilized to script and execute routine maintenance activities that can be automated to save valuable administrator time. PowerShell also provides the ability to execute bulk jobs, or break tasks down into stages in order to achieve a more verbose level of control over virtualization management tasks.

System Center Virtual Machine Manager Self Service Web Portal

The System Center Virtual Machine Manager Self Service Web Portal is intended to provide distributed access to IT personnel outside the core administrative group (see Figure 8.30). This self-service point of access can be permissioned in order to safely provide virtual environment access to development teams to perform their required tasks, without providing them full administrative access to the system. Virtual machine templates can then be used to allow development team type users to manage their own virtual asset requirements in a controllable manner.

Figure 8.30 The System Center Virtual Machine Manager Self Service Web Portal



Virtual Machine Manager Library

The Virtual Machine Manager Library is a subcomponent of Virtual Machine Manager 2007 that serves as a repository of all virtual machine— and virtual environment—related data storage. The main types a material stored in this repository would be the following:

- **Virtual Machine Deployable Images** Used to rapidly deploy production or development VMs
- **Virtual Machine Deployment Templates**

- **Operating Systems .ISO Files** Used for installation to new VMs
- **VHD Virtual Machine Disk Files**

The Library is created during the initial setup of the Virtual Machine Manager Console. The administrator is prompted for a file share, which must be configured and available for the process to complete. After that, the administrator who designates this subject file share as the library repository, and Virtual Machine Manager then proceeds to automatically detect and organize all assets discovered within this share.

For companies with geographically distributed locations to be serviced, the library can be structured in such a way as to allow for multiple repositories which can share their content with remote sites quickly easily.

Migration Support Functionality

System Center Virtual Machine Manager provides the functionality to scan physical server assets for key indicators, and generate a consolidation recommendation based upon a server's assessed suitability for consolidation on to a virtual platform.

To accomplish this, it uses a combination of historical performance data stored in System Center Operations Manager. Unfortunately this means that the full functionality of this feature may not be available to organizations that have not deployed the System Center Operations Manager application in parallel with System Center Virtual Machine Manager.

A critical task in any effort to migrate to a virtualized environment is the ability to preserve and reutilize existing production or development application assets in order to avoid loss of time, administrative effort, and ultimately money that was spent to create those application assets in the first place. Rebuilding a new virtual server, and then reinstalling, and reconfiguring every single application, and server functionality deemed to be appropriate for virtualization would not only be incredibly wasteful, in many cases it would be impossible. The logistics alone of attempting to organize and accomplish a large migration in this manner, in a production environment would be daunting to say the least.

For this reason, the capability has been developed to take already built, configured, and running application assets, and convert them on the fly into a format suitable for deployment into a virtual environment. This process and technology has been universally labeled throughout the industry as (P2V) or physical-to-virtual, and many vendors have developed their own versions of this technology and process because of the significant demand for this capability. For our purposes here, however, we are speaking about the solution offered specifically by System Center Virtual Machine Manager.

In System Center Virtual Machine Manager 2007 this P2V tool and its functionality have been integrated into the Management Console and is an included component in the Virtual Machine Manager Software package. This version uses Microsoft's Volume Shadow Copy Service as the underlying engine used to accomplish the conversion.

A step-by-step wizard has been provided to make the process easy to accomplish. As with everything related to System Center Virtual Machine Manager's functionality, this P2V process is accessible via PowerShell, and can be scripted to run with more verbose functionality options as desired. First, the process can be scripted and set up to run batch jobs in order to accomplish bulk conversions in a large-scale migration scenario. The process can also be broken down into its stages with the use of PowerShell scripting in order to maintain greater control over the migration process.

The stages of this process from start to finish are as follows:

- Enumerate source physical server files, create an image from this source.
- Convert that image to .vhf format and prepare it for deployment to a virtual machine.
- Create the final virtual machine on the target host using the .vhf file.

System Center Virtual Machine Manager also has the necessary functionality included to perform physical-to-virtual conversions on the VMware-based .vmdk file format. This has been done in order to allow customers who wish to convert their virtual assets from the VMware platform to the Microsoft virtualization platform to do so easily. This process is labeled as the virtual-to-virtual conversion (V2V). This is also an industry-standard label for this process, as is the case with (P2V).

Virtual Machine Creation Process Using SCVMM

As seen earlier in Exercise 8.2, virtual machines can be created locally on any instance of Windows Server 2008 running the Windows Server Virtualization (WSv) Role; however, it is Microsoft's intention that the System Center Virtual Machine Manager Console be utilized as the desired enterprise management solution for Windows Server-based virtual assets.

At the time of this writing the process of virtual machine creation process for Windows Server 2008-based virtual assets using System Center Virtual Machine Manager 2007 is still in beta format. This means that a complete and accurate list of expected functionality has not yet been confirmed and finalized.

Managing Servers

There are several options available for managing virtual assets in a Windows Server 2008 Virtualization environment.

- **Windows Server 2008 Virtualization Management Console – Stand-Alone Version**
 - This is the default tool installed with the Windows Server Virtualization Role.
 - Available locally on a full install of Windows Server 2008.
 - Must be accessed from a remote server with a full installation of Windows Server 2008, or a Windows Vista-based workstation for a Server Core installation.
 - The remote server must have the Windows Server Virtualization Role installed in order to have this console available.
- **Server Manager – Roles – Virtualization Management Console**
 - This provides functionality that is almost identical to Windows Server Virtualization Management Console.
 - Available locally on a full install of Windows Server 2008.
 - Must be accessed from a remote server with a full installation of Windows Server 2008, or a Windows Vista-based workstation for a Server Core installation.
 - The remote server must have the Windows Server Virtualization Role installed in order to have this console available.
- **Systems Center Virtual Machine Manager 2007**
 - This previously discussed management interface provides the most verbose set of virtual asset management options available for Windows Server 2008-based virtual assets at this time.
- **PowerShell command line utility**
 - Provides verbose scripting capabilities to carry out common repetitive tasks.
 - PowerShell scripts can be scheduled to automatically perform repetitive routine maintenance on virtual assets.

- **WMI Interface**

- Provides an alternative method for carrying out scripted management tasks.

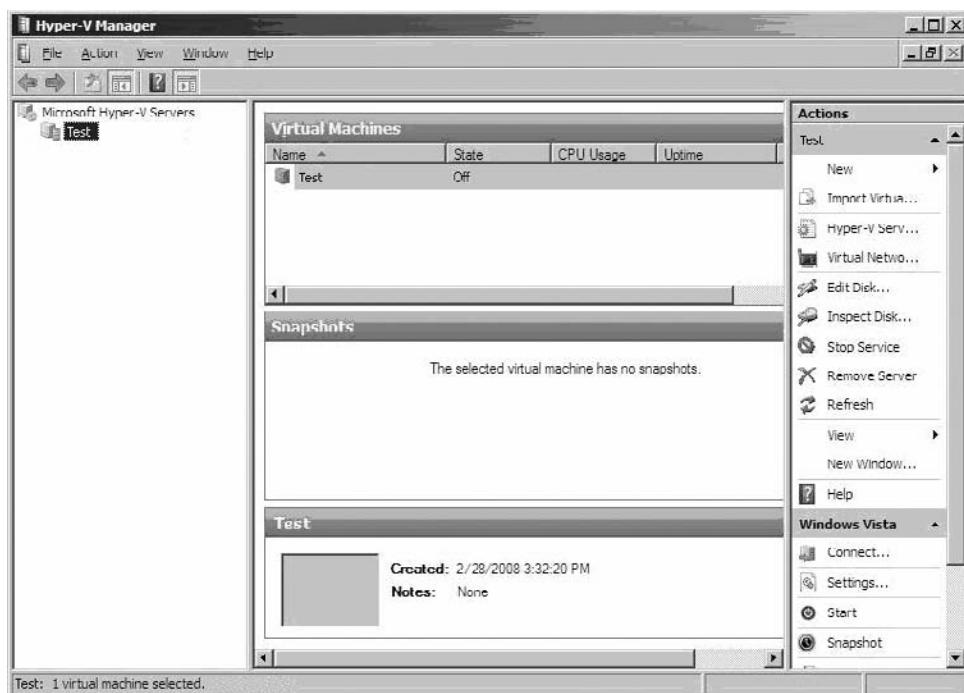
Stand-Alone Virtualization Management Console

Windows Server 2008 includes an MMC management tool called Virtualization Management Console. While this tool is specific to Windows Server 2008, it does share many similarities with System Center Virtual Machine Manager 2007 Console (see Figure 8.31).

This is mainly because they are both designed according to the common Microsoft standard format of Hierarchy on the left, content in the middle, and tools, and tasks to the right side.

As is the case with the previously discussed System Center Virtualization Manager 2007 Console, there is a familiar thumbnail view of the selected virtual machine's console in the lower right pane. The same functionality of double click on the thumbnail to open the console exists within this management console as well.

Figure 8.31 The Stand-Alone Virtual Machine Manager Console



Managing Applications

Microsoft acquired a company called Softricity back in July 2006. As part of that acquisition, they also acquired an interesting new solution called SoftGrid Application Virtualization. This idea behind this piece of technology is to virtualize the application itself, rather than the underlying operating system. The theory is that an application contained in this format would never actually be installed on the target computer, but rather could just be hosted as a guest on any desired computer, regardless of where that computer or its intended user might be located. This allows for the deployment of such applications throughout an organization in a highly dynamic manner. This technology also has the potential to allow dynamic updates and changes to such applications to be delivered to domain members in a Windows Server environment in a policy-based administration model.

Because a virtualized application is also prevented from actually writing to the registry or system files of the underlying O/S, the system is protected from not only potential system destabilization that might be caused by things such as problem .dll but also the potentially degrading effects upon the host O/S of repeatedly application installations, and uninstalls over time due to normal upgrade, and update activity.



TEST DAY TIP

While the virtualized application is prevented from writing to the registry and system files of the underlying O/S, it is able to read these key system files in order to facilitate interaction between virtualized applications, and locally installed application like Outlook for example.

Although SoftGrid is a server-side technology, the intended target for the deployment of these virtualized application images is more the workstation end of the spectrum rather than server-based applications. The current thinking is that this technology could revolutionize the way in which applications are deployed to desktop users within an organization. At the time of this writing this technology has not yet been integrated into the Windows Server 2008 domain model, but it is a technology to watch out for, as Microsoft works to develop it into an integrated solution for future releases.

The most significant advantages offered by this technology include the following:

- **Application Conflicts** Prior to the advent of Application virtualization whenever two or more potentially conflicting applications were required to coexist on the same desktop O/S items such as differing required Java versions, etc. could lead to big issues. The use of SoftGrid technology effectively isolates these applications from one another, meaning that they can be now be run on the same workstation, each running their own specific requirements independently of each other.
- **Multiple Versions of the same application** In a scenario where multiple versions of an application such as MS Word, and MS Access were required to be run simultaneously on a single workstation in order to provide support for legacy file versions, etc, SoftGrid can provide an ideal solution. With the differing versions of the subject program virtualized, they will run in an isolated manner, effectively removing any limitations on their cohabitation.
- **Terminal Services Compatibility** Many applications simply do not function well, or at all when run on a Terminal Services platform. With the level of isolation provided by application virtualization, this limitation can be effectively removed. What this means to administrators who deploy applications via terminal services solutions is that non-Terminal Services compatible programs be now be effectively deployed via Terminal Services. As well applications that previously required separation into different terminal server application silos for compatibility reasons, can now be deployed together.
- **Workstation O/S Reduced Maintenance** Since SoftGrid creates a layer of isolation between the O/S, and application level, there is nothing actually installed on the workstation to affect the registry, and other key system files. In the past, multiple installs, and uninstalls of differing applications over time would often result in the registry becoming highly cluttered with unwanted information. Not to mention many other system files that might become overfilled with necessary information wasting space, and system resources. The result would be that workstations would periodically required rebuilding, just to clean up the after affects of these sorts of activities. With the deployment of a SoftGrid solution, the workstation O/S could be left alone to run clean, and potentially trouble free for a much longer period of time than was previously possible.

- **Application Deployment and Maintenance** As mentioned previously, since a virtualized application can be dynamically deployed from a centralization server-based source, it will no longer be necessary to manually visit workstations, to install, or uninstall applications with every update, or upgrade. Essentially, every time that a user accesses an application, they will be getting the latest, most up to date version streamed to their desktop from the central server. An advancement that will serve to dramatically improve overall administrative efficiency and effectiveness.

The way that the application streaming format used by SoftGrid works is that a Microsoft System Center Virtual Application Server maintains the configured virtual applications. When accessed by a user, the application is streamed to the user's desktop, caching the most critical required components at the workstation level until enough of the application's core required content is present on the workstation to launch it. The percentage of content required to actually launch an application during streaming would normally be about 10 to 30 percent depending on the specific application. This core 10 to 30% content remains cached on the workstation, with additional content being called from the central server on an as required, as accessed basis. Once cached, the application will not require the restreaming of this initial core content on subsequent user accesses, unless there is an update or an upgrade provided at the central server that needs to be restreamed to bring the application's content up to date.

NOTE

For the initial streaming of required core application content, and slight delay of 5 to 15 seconds may be experienced by the user, however once cached, there should be no delay in application launch performance.

TEST DAY TIP

The solution to traditional application compatibility problems is considered to be one of the most significant benefits offered by SoftGrid's application virtualization offering.

SoftGrid has direct integration with Active Directory, meaning that every client access is authenticated. Additionally the direct integration with AD means that granular control can be placed over things such as application license allocation limits, etc.

There are seven core components required for the deployment of a SoftGrid Application Virtualization solution. They are as follows:

- **SoftGrid Sequencer** The Sequencer is a key piece of software that is used to package the applications to be virtualized into a format that the virtual platform can read, and execute. A GUI-based wizard process is provided in which the administrator is asked to go through the motions of installing and configuring the subject application, in the same manner that would be done if he or she were installing it on an autonomous system. The output of this process is a set of files that are then deployed to the System Center Virtual Application Server as the content to be streamed out to waiting clients.

NOTE

The task of sequencing an application in preparation for its deployment as a virtualized application is considered to be a somewhat intricate and involved process. Administrators looking to deploy applications therefore benefit greatly from proper training and experience.

- **Microsoft System Center Virtual Application Server** The job of the System Center Virtual Application Server is to store, and distribute the application content to the clients when requested. It also handles the communication of authentication requests between the clients and Active Directory.
- **Data Store** SoftGrid does maintain a relatively small, low transaction database containing all configuration information. The resource requirements for this database are not high, and either MS SQL or MSDE can be used to satisfy this requirement.
- **Management Console** The Management Console is used to control all SoftGrid-based assets.

- **An Authentication Source (Active Directory or other)** Since all client access requests are authenticated, it is necessary to have connectivity to an authentication source such as Active Directory. Legacy NT4 style Domain Authentication will work as well, but I suspect that demand will be limited for this particular feature.
- **SoftGrid Clients** There are 2 versions of the SoftGrid Application Client?
 - **Desktop Clients** The SoftGrid Desktop Client is an Agent that gets installed on the target workstation's O/S, in order to provide the needed communication link between the client and the System Center Virtual Application Server
 - **Terminal Services Clients** The SoftGrid Terminal Services Client is an Agent that gets installed on the Terminal Server that is presenting the subject applications. As is the case with the Desktop Client, its purpose is to provide the needed communication link between the Terminal Services Client and the System Center Virtual Application Server

Refer to the Microsoft Web site for more detailed information on this highly intriguing new virtualization offering.

Managing VMware

Microsoft has promised to include support for VMware, not only through their System Center Virtual Machine Manager Server 2007, but also in the underlying PowerShell command line scripting functionality that the entire System Center Virtual Machine Manager Application is built upon. The goal is to allow for easy Migration from the VMware platform with its .vmdk file format, to Microsoft's Windows Server Virtualization platform with its .vhdx file format, for those who wish to do so.

A wizard-based virtual-to-virtual (V2V) conversion tool for VMware-based virtual machines is available under the Administrative Console of System Center Virtual Machine Manager Server 2007. This tool is designed to provide easy conversion from the .vmdk format to the .vhdx file format utilized by Windows Server Virtualization.

As always with System Center Virtual Machine Manager 2007, there is full PowerShell support for this task to be carried out at the command line. PowerShell can also be used to carry out bulk conversions. This conversion process requires that the source .vmdk be offline, but the P2V process can be used to convert VMware-based VMs that are online.

The .vmdk file formats that are supported by this migration capability are as follows:

- vmfs
- monolithicSparse
- monolithicFlat
- twoGbMaxExtentSparse
- twoGbMaxExtentFlat

At the time of this writing the full functionality of the Windows Server Virtualization Manager is not known as it is still in pre-release status. While the V2V functionality for VMware-based virtual assets using the .vmdk file format will be available through the promised upgrades to System Center Virtual Machine Manager, it is not yet known whether or not this same functionality is planned to be offered through the Windows Server Virtualization Manager Console. What Microsoft has said is that they are planning to make the .WMI Interface code readily available to all other organizations who wish to develop customer solutions of their own.

As well, support for the ongoing management of VMware-based virtual machines has been promised as a feature that will be included in the final release of System Center Virtual Machine Manager 2007. This would obviously make it much easier for organizations running on mixed platforms to make good use of the Microsoft System Center management package to achieve a unified enterprise management solution. Once the final release has been made available to the public it will be easier to determine the true extent to which this unified virtual asset management solution will be possible.

Summary of Exam Objectives

Microsoft has made a bold move forward with its new Microkernel style Hypervisor design. A clear departure from previously employed emulation, and Monolithic style Hypervisor architectures the Microkernel design promises greatly improved security for guest VMs from malicious code attacks as well as advancements in overall system stability via the removal of the device drivers from the hypervisor layer in this design. The new Hyper-V virtualization model also provides interesting options with respect to areas such as server workload consolidation, Laboratory environment creation and maintenance, and Disaster Recovery solutions. The later being especially true when Hyper-V technology is deployed in concert with other intriguing options such as Windows Server 2008-based failover clustering solutions. The marriage of these two technologies promises to provide options for low cost, and highly recoverable, and flexible solutions in this area that have never before been possible.

The promised integration with the upcoming release of the next version of System Center Virtual Machine Manager 2007 expected to coincide with the final release of Hyper-V in mid-2008 will add a great deal of weight to Microsoft's overall virtualization offerings. SCVMM 2007's verbose enterprise level management functionality is highly complimentary to the Hyper-V feature set, and together they will form a highly capable virtualization solution. Its capabilities include the well designed ability to easily perform functions such as P2V, rapid virtual machine creation from templates, and .iso files stored in the library. As well SCVMM 2007's close integration with System Center Operations Manager will provide the virtual asset performance monitoring capabilities that are so critical to enterprise level clients. To add to all this, Microsoft has made the decision to include support within SCVMM 2007 for VMware-based virtual assets as well. A wise decision I believe, as it will not only allow for the management of mixed Hyper-V, and VMware-based environments, but will also facilitate the smooth and easy transition and migration of VMware-based assets over to the Hyper-V platform for those who choose to do so.

It seems that with the current state of the offerings from different competitors, Microsoft's integrated management solution, based on their System Center product line may be their greatest asset to be played against the well established market share of the VMware platform. With all industry contenders working diligently to catch up to the product maturity level advantage that VMware currently enjoys, it will certainly be interesting to see where this technology will take us in times to come.

Exam Objectives Fast Track

Understanding Windows Server Virtualization and Consolidation Concepts

- Virtualization is a technology that allows many autonomous operating systems to be run in isolation from one another, while utilizing the same physical hardware. Windows Server 2008 Hyper-V uses hardware assisted virtualization technology. It therefore requires the support of 64-bit processors that contain specific functionality improvements.

Windows Server 2008 Hyper-V uses microkernel hypervisor architecture. This new style of hypervisor provides reduces vulnerability to attack from hackers, as well as reduced susceptibility to system instabilities that might be caused by code issues with drivers.

The design of the microkernel hypervisor requires the assistance of the processor to facilitate certain portions of the communication between the virtual machines and the underlying physical hardware. Also processor support is required for a new security feature called Data Execution Prevention (DEP).

- Virtualization allows for multiple server roles to be consolidated onto one or at least fewer virtual server workloads greatly improving efficiency. The key is in the proper selection of candidates for consolidation. It is normally not wise to consolidate functions whose roles are of critical importance to the organization, since maintenance activities to one workload could adversely affect another. Sometimes functionalities need to be maintained on separate workloads in order to ensure their availability throughout the enterprise. Also, virtual platforms do run a slightly higher risk of temporary outage due to activities such as the need to migrate from one host to another, and therefore applications that have a zero tolerance to downtime are generally not good candidates for virtualization and consolidation.

The design of the microkernel hypervisor requires the assistance of the processor to facilitate certain portions of the communication between the virtual machines and the underlying physical hardware. Also processor support is required for a new security feature called Data Execution Prevention (DEP).

Installing and Configuring Windows Server Virtualization

- The prerequisites for installing the WSV Role are updating the BIOS, enabling the needed features in the BIOS, and then installing the Hyper-V RC0 update KB949219. Only after these prerequisites have been met can you successfully install the WSV Role. If the .msu updates are not installed, then the WSV Role will not be available for selection and installation under the **Server Manager | Roles** pager, and if the BIOS settings are not enabled, then HYPER-V will not start after installation.
- Once the Hyper-V Role has been installed on a Server Core instance of Windows Server 2008, it is necessary to connect to it from another server running either a full install of Windows Server 2008, or a Windows Vista computer running the appropriate tools for WSV Role management. A Server Core installation does not have the Server Manager GUI tool. Server Roles cannot be installed through Server Manager while connected remotely to another Windows Server 2008 instance. Roles can only be installed while connected locally.
- On a Server Core install of Windows Server 2008 the WSV Role must be installed locally at the command line by typing the command: **Start / w ocsetup Microsoft-Hyper-V**.
- After the WSV Role has been installed the Windows Server Virtualization Manager snap-in will be available from two locations.
- Server Manager | Roles | Windows Server Virtualization**
- The Stand-Alone **Windows Server Virtualization Manager**
- New virtual machines can be configured as per the following constraints:
- For the **guest operating system**, the following are the currently supported options:
 - Windows Server 2008** (all 32-bit and 64-bit versions)
 - Windows Server 2003** (all 32-bit and 64-bit versions)
 - SuSE Linux Enterprise Server 10 SP1** (beta x86 and x64 editions)
- For the assignable system resources, the following are the available options:
 - Up to 64Gb memory per VM
 - Up to 4 virtual SCSI disks per VM

- Up to 8 processors per VM
- Up to 8 virtual network adapters per VM

Learning about System Center Virtual Machine Manager 2007

- Virtual Machine Manager Server is a core application. It utilizes a SQL Server 2005 database to store all virtual machine related metadata. It runs on either 32-bit or 64-bit version of Windows 2003 Server. It is designed to manage Microsoft-based virtualized resources in the .vhf format. It does possess the additional ability to convert VMware-based .vmdk format files into the .vhf format.
- The VMM Server can be accessed through any of the following interfaces:
 - Virtual Machine Manager Administrator Console
 - Self Service Web Portal
 - Windows PowerShell Command Line Utility
- System Center Virtual Machine Manager currently possesses the capability to perform virtual machine management for the following Virtualized assets:
 - Microsoft Virtual Server R2-based virtual assets
 - Microsoft Windows Server 2008 virtual assets (full capability promised in next release)
 - VMware-based virtual assets (not yet available, but functionality is promised in next release)
- The Virtual Machine Manager Library serves as a repository of all Virtual Machine and Virtual Environment related data storage. The main types a material stored in this repository would be:
 - Virtual Machine Deployable Images
 - Virtual Machine Deployment Templates
 - Operating Systems .ISO Files – Used for Installation to New VMs
 - VHD Virtual Machine Disk Files

- Every VMM task and tool has a corresponding Windows PowerShell command, which can be viewed during execution. PowerShell can also be used directly to script and execute routine maintenance activities that can be automated to save time. PowerShell also provides the ability to execute bulk jobs, or break tasks down into stages in order to achieve a more verbose level of control over virtualization management tasks.

Learning to Manage Windows Server Virtualization-Based Assets

- There are several options available for managing Virtual assets in a Windows Server 2008 Virtualization environment:
 - The Windows Server 2008 Virtualization Management Console
 - The Server Manager – Roles –Virtualization Management Console
 - System Center Virtual Machine Manager 2007
 - The PowerShell Command Line Utility
 - The WMI Interface
- Microsoft has promised to include support for VMware, not only through their System Center Virtual Machine Manager Server 2007, but also in the underlying PowerShell command line scripting functionality. At the time of writing this remains a promise, but the expected functionality is that VMware-based virtual assets will be directly manageable through the SCVMM 2007 Management Console. As well, there will be support for the virtual-to-virtual (V2V) conversion utility, designed to allow customers to migrate their virtual assets over to the Microsoft platform.
- Microsoft has recently acquired a new technology called SoftGrid Application Virtualization. Its purpose is to virtualize the application itself, rather than the underlying operating system. The idea is that an application contained in this format would never actually be installed on the target computer, and could be hosted as a guest on any desired computer. This would allow for the deployment of applications throughout an organization in a highly dynamic manner. Dynamic updates and changes could then be delivered in a policy-based administration model. The intended target for this is more the workstation end of the spectrum.

Exam Objectives

Frequently Asked Questions

Q: I have developed a server consolidation plan based upon the application workloads that I believe are best suited for virtualization and consolidation but I'm not sure if the criteria that I applied to the selection process are correct. How can I be sure?

A: Ensure that this plan includes considerations for the criticality of the assessed workload's application or functionality. In general, workloads that require redundancy or geographically dispersed servers in order to ensure the availability of a particular function should be avoided in any virtualization plan. As well, applications or functions determined to be sufficiently critical that they can not tolerate even a short period of outage are not good candidates for consolidation.

Q: I have a significant problem with an older-but critical-business application that my desktop users depend upon that will not run on the newest desktop operating system being used in my company. To further complicate the situation, there are several other business critical applications also running on our workstations that will only run on this newer operating system. How can I find a solution that will allow me to deploy both the application with legacy O/S requirements, simultaneously with the newer applications to my desktop users?

A: An application such as this with a dependency on a legacy operating system is often a prime candidate for the SoftGrid Application Virtualization solution. With SoftGrid an application such as this can be virtualized and seamlessly delivered to the desktop user, regardless of what O/S his or her workstation is running. With this solution applied, the security and application support requirements for the newer O/S can be satisfied, while simultaneously satisfying the requirement to support the legacy application.

Q: I am trying to develop an integrated and unified solution to suit my company's needs and satisfy its requirements for the management of its virtualized assets. How can I know if I am making the right choices regarding individual virtualization management products?

A: The answer to this question depends upon many factors. First, the size of an organization is a significant determining factor in what level of virtualization management solution should be deployed. For an organization only looking to satisfy their quality assurance, development, or disaster recovery requirements,

the native management tools included with Windows Server Virtualization would most likely prove sufficient. In this situation the investment in enterprise level management tools would not really be practical. For a large organization however, the more verbose functionality offered by System Center Virtual Machine Manager 2007 would be more appropriate. When coupled with System Center Operations Manager, these two components of the System Center product line can provide the unified and integrated solution for the enterprise level management not only of virtual assets, but of physical server assets as well. The system health and status monitoring capability of System Center Operations Manager can allow administrators to stay on top of all issues, and handle them proactively. There is also the ability to collect, and display performance data, both current and historical that can be a vital component in server placement and resource allotment decisions for virtualized assets,

Q: I have developed a set of standards to be used by my company to determine the ideal placement of virtual servers after they have been virtualized and or consolidated. How can I know if these standards are correct, and if the result of these server placement decisions is having the desired effect?

A: As previously mentioned System Center Operations Manager is a vital component in this process. System Center Virtual Machine Manager 2007 provides the tools necessary to make good decisions regarding which hosts are the best candidates for virtual machine placement, but these tools depend upon the performance data that would traditionally be stored in System Center Operations Manager. As a result, these two products should be seriously considered for parallel deployment in order to realize the full capability of System Center Virtual Machine Manager 2007.

Q: I am running a mixed environment with VMware-based virtual assets running along side Windows Server Virtualization-based virtual assets. How can I ensure that I can manage these assets effectively?

A: Microsoft has promised that the next production release of System Center Virtual Machine Manager will be able to cross manage VMware-based virtual assets. This release is scheduled to coincide with the production release of Windows Server 2008 Hyper-V in mid-2008. This will allow for a unified enterprise management solution for the management of virtual assets in any mixed environment. There is also the capability from SCVMM to perform virtual-to-virtual conversions of VMware-based virtual machines using the .vmdk

file format over to the .vhdx file format utilized by Hyper-V. As a result of this capability the option does exist to migrate all non-Hyper-V-based assets over to the same format, in order to achieve a unified solution, not only for VM management, but also for virtual environment architecture, and so on.

Q: I need to design a strategy to execute a migration to virtual platforms for the workloads that have been determined to be appropriate. What process should I follow?

A: Normally, the P2V functionality is the primary tool utilized to perform this function. The V2V may be part of the migration strategy if a migration from VMware to the Hyper-V platform is a part of the determined requirement. Other than this, however, after building a list of good workload candidates targeted for virtualization, the P2V tool can be used to create a virtual copy of the physical source server. The newly created virtual copies can have their names altered slightly, in order to allow them to coexist on the network in parallel with the original. Once the application owners have validated the functionality of the new VM, a controlled cutover can be carried out.

Self Test

1. The hardware specific requirements for Windows Server Virtualization include processors with which feature included?
 - A. eXecute Disable memory access support
 - B. Data Execution Prevention
 - C. Virtual data execution protocol.
 - D. Monolithic hypervisor protocol support
2. Additional processor specific hardware functionality improvements for Windows Server Virtualization are required for which two reasons? (Choose two answers.)
 - A. Support for eXecute Disable memory access support
 - B. Support for additional security features
 - C. Enhanced performance characteristics for guest operating systems.
 - D. Assistance with hardware communication for guest operating systems
3. Operating System Enlightenments apply to which partitions in Windows Server Virtualization architecture?
 - A. The parent partitions only
 - B. Both parent and child partitions
 - C. Child partitions only
 - D. The drivers running in the hypervisor layer
4. Virtual Service Providers run in which part of the Windows Server Virtualization architecture?
 - A. In the Kernel Process layer of the parent partition.
 - B. In the User Process layer of the child partition.
 - C. In the User Process layer of the parent partition.
 - D. In the Kernel Process layer of the child partition.
5. VM Worker Processes run in which part of the Windows Server Virtualization architecture?
 - A. In the Kernel Process layer of the parent partition.
 - B. In the User Process layer of the child partition.

- C. In the User Process layer of the parent partition.
 - D. In the Kernel Process layer of the child partition.
6. VSP/VSC Pairs are used to accomplish what function in Windows Server Virtualization architecture?
- A. They allow for memory to be reserved for exclusive use by the guest operating systems.
 - B. They allow the parent partition to communicate with child partitions which are running operating systems that have no enlightenments.
 - C. They allow the parent partition to support a longer list of legacy O/Ss.
 - D. They are used for communication of hardware access requests between the child and parent partitions across the VMBus.
7. Which of the following are prerequisites which must be in place to support an instance of Windows Server Virtualization? (Choose all that apply.)
- A. Physical hardware running 64-bit processors
 - B. Physical hardware running processors which support Data Execution Prevention (DEP) technology
 - C. A minimum of 32Gb of memory
 - D. Windows Server 2008 Server Core installation
8. Which benefits can directly be associated with a move to virtualization in a data center? (Choose all that apply.)
- A. Improved IT administrative efficiency
 - B. Reduced power consumption
 - C. Reduced cooling costs
 - D. Faster disk access times
9. In a microkernel-style hypervisor model, in what partition component does the virtualization stack run?
- A. In the Kernel Process layer of the parent partition.
 - B. In the User Process layer of the child partition.
 - C. There is no virtualization stack in a microkernel hypervisor.
 - D. In the parent partition.

10. In a monolithic-style hypervisor model, what partition is used for Administrative Console access?
 - A. In the parent partition.
 - B. In one of the child partitions.
 - C. In one of the guest partitions.
 - D. The Administrative Console is not accessed through any of the partitions in monolithic hypervisor architecture.

Self Test Quick Answer Key

- | | |
|----------------|-------------------|
| 1. B | 6. D |
| 2. B, D | 7. B |
| 3. C | 8. A, B, C |
| 4. A | 9. D |
| 5. C | 10. C |

This page intentionally left blank

Chapter 9

MCITP Exam 647

Planning for Business Continuity and High Availability

Exam objectives in this chapter:

- Planning for Storage Requirements
- Data Collaboration
- Planning for High Availability
- Planning for Backup and Recovery

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

A major concern for any organization these days is the maintenance of the safety and security of their data resources. Organizations these days invest huge sums of money to develop and maintain the intellectual content needed to function in modern business. In many cases this intellectual content can comprise the very essence of what makes a particular company what it is. Safeguarding this intellectual content can therefore be critical to an organization's survival.

Many methods and technologies to safeguard these resources include implementing solutions like the following:

- **Hardware redundancy** Hardware redundancy server to protect data assets by preventing potential data losses which might result from an event such as a failed hard drive or power supply. By providing multiple hard drives and power supplies, as well as other similar mission-critical hardware configured to fail over in a redundant manner should anything fail unexpectedly, important data can be effectively protected.
- **Data redundancy** By deploying solutions such as Distributed File System which is designed to automatically replicate data to multiple locations on multiple hardware platforms, data can be effectively protected from potential loss caused by any unforeseen issue which might affect a specific server or site.
- **Dynamic backup** A dynamic backup solution can be used to protect an organization's data assets on many levels. In the event of the failure of specific hardware, a well-thought-out backup solution can be used to recover easily regardless of what the degree of loss might be. Whether it's one server that has failed, or an entire site that has been destroyed by a natural disaster, well-planned backups, with off-site storage solutions included, can make the difference between rapid recovery and serious problems after the unexpected has occurred.
- **Disaster Recovery Solutions** A solid, well-planned, and practiced Disaster Recovery solution is the cornerstone of any organization's solution to protect itself against potential data losses caused by unforeseen events such as power outages, severe storms, etc. Disaster Recovery solutions normally involve redundant hardware running at a mirrored site, in a geographically separated location from the organization's main IT assets. This represents the highest level of protection for an organization, designed

to protect it not just against losses resulting from problems with a specific piece of hardware, but more so from the loss of an entire site for one reason or another. Without an effective DR plan in place, a company could find itself out of business in the wake of an unexpected catastrophic event.

All of these key infrastructure components are designed not only to ensure that an organization can maintain consistent reliable access to their data resources, but that they can recover quickly and regain access to those resources in the wake of any unforeseen event. You may remember that not such a long time ago many organizations lulled into a false sense of confidence by the reliability of North American infrastructure were shocked out of their complacency by a large scale power outage that affected a huge area surrounding the Great Lakes region. This event represented a validation for those companies who had taken the time, energy, and expense to properly prepare for such an event, and a hard lesson learned for those organizations who felt overly confident that such planning and expense was not justifiable since something like that would never happen in our modern world.

Inevitably, the infrastructure, applications, and data resources of any modern organization are critical components, without which they cannot do business. Failure to properly plan and implement solutions to ensure the ongoing availability of these critical components could easily prove to be a fatal error for any shortsighted organization banking on the probability that the worst case scenario is something that will never happen to them. Much like life insurance for an individual, you pay into it all of your life, with no visible return for this investment, yet when the one day comes that you do need it, if it's not there, the effects can be nothing less than devastating. In this chapter we will look into some of the newest offerings from Windows 2008 Server technology designed to address these concerns and provide support for the much-needed components of this insurance policy that forward-thinking organizations are demanding these days.

Windows 2008 Server offers some interesting new capabilities in the area of clustering, protections against malicious intrusions, as well as functionality designed to prevent data losses from volume corruption, and other such frustrations all too familiar to experienced administrators.

Planning for Storage Requirements

There are many new storage-related improvements in Windows 2008 Server. Here we will talk about the most noteworthy, with an emphasis on those features which add specific benefit to high availability solutions.

Self Healing NTFS

Any administrator who has been in the IT field for any period of time has experienced the dreaded corrupt data volume scenario. This can be made even worse when this situation occurs on a volume accessed by executive level users who will inevitably expect inhuman results in any efforts to recover from the situation. The reality is that running checkdisk on a corrupted volume of any appreciable size can take a seemingly endless number of hours. These would be long painful hours during which every affected user will undoubtedly be screaming for fast resolution. Windows 2008 Server has included a redesigned version of NTFS, called Self Healing NTFS. It is specifically intended to reduce, if not eliminate, these unpleasant scenarios in the future.

Self Healing NTFS can recover a volume when the boot sector is readable, but the NTFS Volume is not. The sequence of events is that NTFS will detect any file corruption, and make an attempt to recover or repair any such files. If recovery or repair proves not to be possible, then the file will be deleted, and the event will be recorded in the Event Log. There are many who might express reservations at the fact that files could be deleted without their knowledge, or against their wishes, but the fact is that if a file is corrupted beyond recovery, then the ability to retain this file will not make it any less corrupt. Corrupt is corrupt. The fact is that most repairs will occur in the background, without the end user ever even knowing that there has been a problem. For those corrupted files so far gone that they do get deleted, this activity can be viewed by administrators in the logs. If the lost file in question turns out to be important enough, well, this is what backups are for. Monitoring solutions such as System Center Operations Manager 2007 can be utilized to manage these sorts of situations appropriately. Operations Manager can be configured to generate an alert in response to the deletion of corrupted files, allowing administrators to scrutinize the deletion.

The option is available to remove the automated functionality of this feature by turning it off. When turned off, NTFS will generate an alert when file corruption is detected, but it will not take action to correct it. In this case, the onus is on administrators to manually act upon the corruption warning using available tools.

To turn Self Healing off run the following command at the command prompt:

```
fsutil repair set c: 0"  
"c" = affected volume  
"0" = off, "1" = on.
```

Multipath I/O (MPIO)

Multipath I/O has been included as an optional feature with Windows 2008 with the intent to support failover redundancy and load balancing solutions. When configured as a failover redundancy solution, its purpose is to provide a critical component in the overall chain of hardware redundancy deployed by organizations to prevent potential data losses, or outages. In this configuration the unexpected failure of the hardware being used to support the connectivity between the server and its data storage will not lead to any interruption of service or connectivity. When configured as a load balancing solution Multipath I/O can be used to share the load of client connections between two or more physical paths, in order to avoid bandwidth saturation of any one path that could lead to reduced or in any way unsatisfactory performance for the end user.

Multipath I/O provides support for the following storage technologies:

- iSCSI
- Fiber
- SAN

To install the Multipath I/O feature select **Start | Administrative Tools | Server Manager | Add Features | Multipath I/O**.

During configuration the following supported options for Multipath I/O Load Balancing Modes of operation will be presented:

- **Failover** With Failover based Load Balancing a primary path is configured to be used at all times, unless it should become unavailable at some point. In the event that the primary should become unavailable, then traffic will be failed over to a configured secondary path. No load balancing takes place with this configuration. It is strictly for the purposes of providing a redundant secondary path in the event of any sort of failure to the primary path.
- **Fallback** Will always prefer the primary, and will only direct to the secondary when the primary is not available. Will always go right back to the primary as soon as it is available again.
- **Round Robin** All available paths will be used in a balanced approach.
- **Round Robin with a subset of paths** Primary paths are specified, and used in a Round Robin balancing manner. Secondary paths listed in decreasing order of preference will only be used when the last of the primary paths becomes unavailable.

- **Dynamic Least Queue Depth** I/O will always use the path with the smallest traffic load on it.
- **Weighted Path** Each path will be assigned a weight, and the path with the lowest number will always be chosen as the priority path. The higher the number, the lower the priority.

The default configuration is *Round Robin* when the storage controller is set for active / active. When the storage controller is set for *Asymmetric Logical Unit Access* the default configuration is *Failover*.

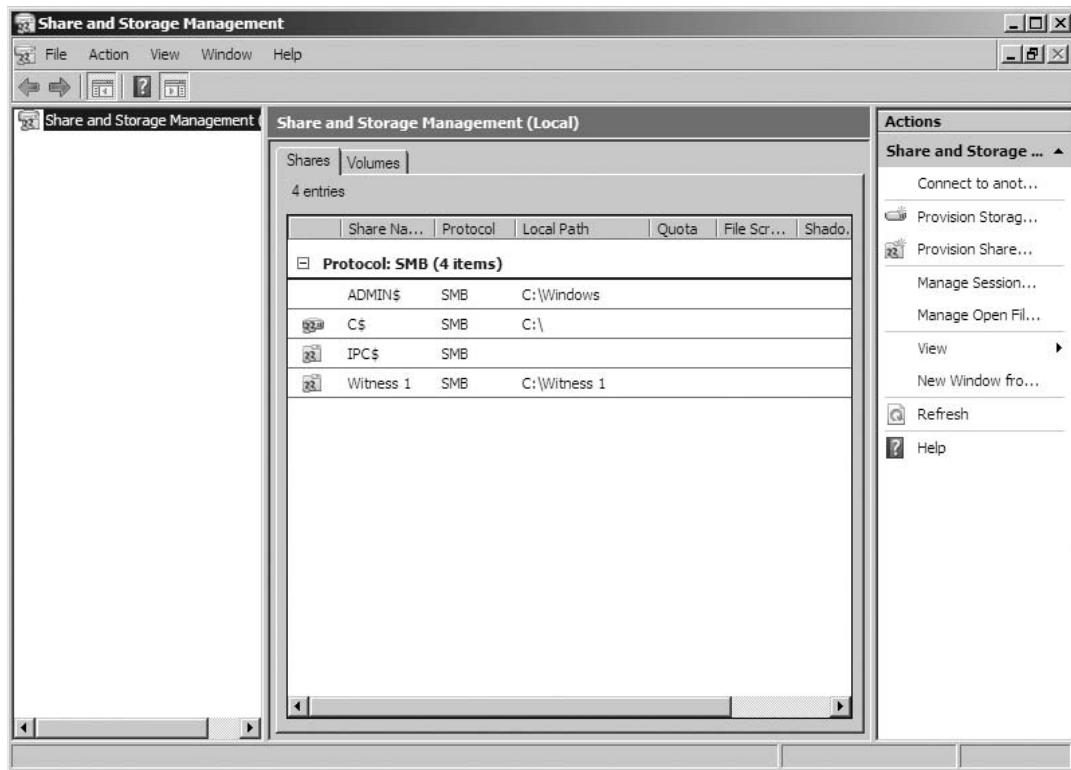
Once installed MPIO can be launched from either of 2 locations: the Control Panel or Administrative Tools. Some storage vendors have their own Device Specific Modules designed to work with W2K8. To install them, open the **MPIO Control Panel Configuration Utility | DSM** tab.

Data Management

Data Management can be defined as all of the individual technologies and functions designed to manage and control data as an overall resource within an IT environment. Within Windows 2008, there could be many different components that could be labeled as being a part of the overall data management solution according to these criteria. Here we will discuss some of the most prominent of these features and functions provided with the new Windows 2008 O/S that are designed to satisfy data management requirements.

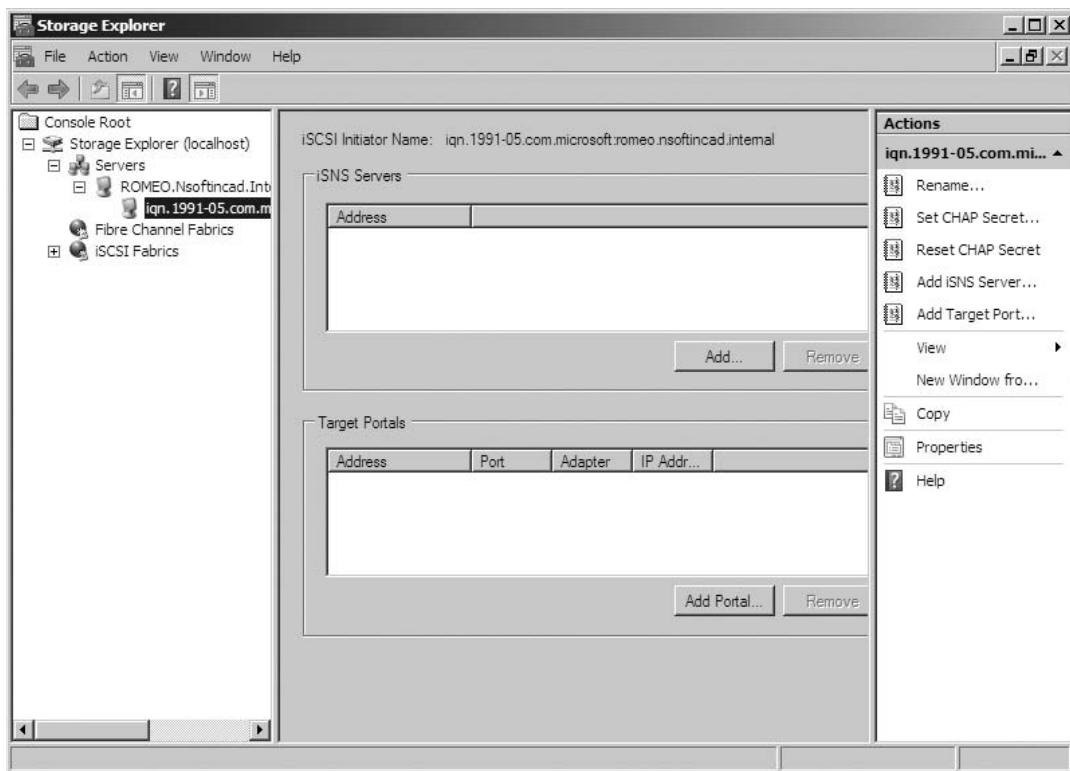
Share and Storage Management Console

The Windows Share and Storage Management Console is designed to give a quick and easy overview of all data shares and volumes on the server instance (see Figure 9.1). This is a much more verbose offering than the very basic **Shares and Sessions** link provided under Computer Management in Windows 2003 Server. It allows for comprehensive control over all share and volume activities on the Windows 2008 Server instance.

Figure 9.1 Windows Share and Storage Management Console

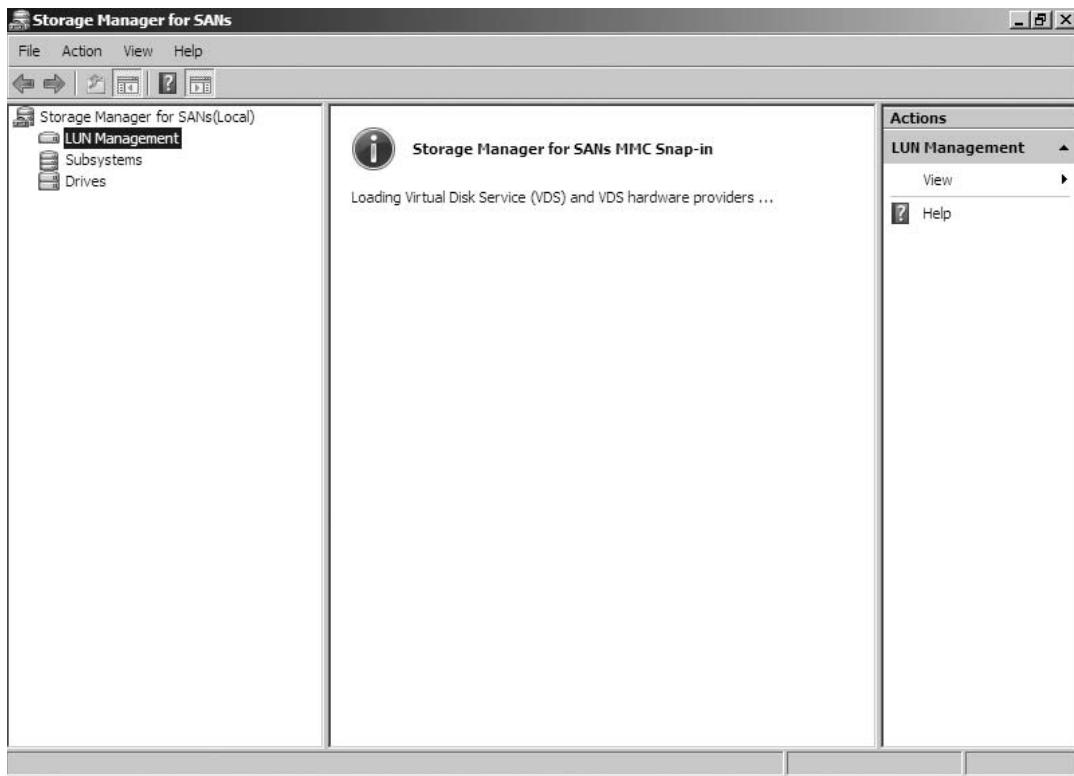
Storage Explorer

The Storage Explorer Console provides a clear overview of all attached SAN, Fiber, or iSCSI storage devices, allowing for easy control and monitoring over these resources (see Figure 9.2).

Figure 9.2 Windows Storage Explorer Console

Storage Manager for SANs Console

The Windows Storage Manager for Storage Area Networks (SANs) Console is an optional feature that is new to Windows 2008, as shown in Figure 9.3. It is designed to give direct and verbose control over all SAN attached assets, including the creation provisioning and formatting of Logical Unit Numbers or LUN Volumes, the component used by the SCSI Protocol to identify its individual SCSI targets. Storage Manager for SANs provides full support for MPIO technology used to provide redundant path solutions for SAN based data storage resources.

Figure 9.3 Windows Storage Manager for SANs Console

Data Security

In answer to the ever-increasing demand for more secure server platforms, Windows 2008 Server has included many new security features. With respect to data security specifically, Microsoft has provided built-in functionality to block and deter attempts at security invasions to critical data resources not just by hackers, but by anyone who could be described as unauthorized. Here we will talk about some of the “standout” new features that have been added with the intent to protect important data from intrusion.

Group Policy Control over Removable Media

As the title suggests, Windows 2008 has included the capability, via Group Policy control, to limit and/or control the use of removable media within an organization's infrastructure. With the advent of ever-increasing capacity in memory key technology, the ease with which critical data can be slipped on to such a device has become a significant security concern. These small memory sticks can often be carried on a key

ring, meaning that they can be used very inconspicuously to extract important files or information without anyone ever noticing.

Head of the Class ...

Securing Memory Keys

You may remember from Chapter 8 where we raised a concern about this very issue with respect to the ability of a person with malicious intent to copy the virtual server file of a Domain Controller in a Lab environment onto one of the newer, larger capacity memory keys and walk out the door with it, completely undetected. This is a very real security threat that should be a concern of any organization.

With this threat in mind, Microsoft has included the following Group Policy setting in Windows Server 2008:

- **Devices: Allowed to Format or Eject Removable Media** The name of this group policy object is self explanatory, and it can be used to prevent the use of specific types of removable media on servers that are subjected to its control.

BitLocker Drive Encryption

BitLocker Drive Encryption is a new feature included with Windows 2008 that is designed to protect the operating system and all data stored on the system volume from malicious activity. By default BitLocker Drive Encryption does not cover data stored on volumes other than the system volume, but it can easily be configured to do so.

It is an optional feature in Windows 2008 Server that can be installed by either two methods:

- **Server Manager** BitLocker Drive Encryption can be installed using the Add Features Wizard under Server Manager Console.
- **Command Prompt** BitLocker Drive Encryption can be installed from the Command Prompt using the following command:

```
ServerManagerCmd -install BitLocker -restart
```

BitLocker is designed to encrypt all files, including paging and hibernation files on all configured volumes in order to block unwanted access by unauthorized parties. It uses something called a Trusted Platform Module (TPM) to encrypt and protect files used during startup, in order to prevent file modification using Pre-execution environment type tools that can be used to modify files when the operating system is not yet running.

BitLocker Drive Encryption has the following prerequisite dependencies:

- Hardware with confirmed support for TPM Version 1.2
- A system BIOS with confirmed support for TPM Version 1.2 and Static Root of Trust Measurement
- The system partition in which the O/S is installed must not be an encrypted partition.

After a volume has been encrypted using BitLocker there will be a slight degradation in performance resulting from the extra processing required for the access to encrypted files from that point forward. This anticipated reduction in performance, although not significant, is still something that should be taken into consideration before implementing BitLocker on heavily loaded systems that are sensitive to factors that might negatively impact performance.

Another point to consider is that once BitLocker has been enabled on a volume, it will no longer be possible to remove the drives from one server and place them into another, since BitLocker will respond to this as an attempt to bypass security by modifying ACLs for the affected files. Since the relocation of drives from one server to another is a common scenario used by administrators to recover data files to an alternate hardware platform in the wake of a hardware failure, or other similar scenarios, the loss of the ability to carry out this sort of action is another factor that should be carefully considered before implementation of BitLocker in any environment.

BitLocker works in conjunction with the previously mentioned TPM hardware support to provide protection for the files used during the startup process. These files would include the following:

- BIOS
- Master Boot Record
- Master Boot Sector
- Boot Manager Code

On startup BitLocker reads the values of these files, and generates a hash value which is then stored in the TMP. This hash value can only be altered on system startup.

There is also the capability to have TMP create a secure key from this hash value that can only be read by that particular TMP, blocking any attempts to start the same files on different hardware. In this scenario, on system startup TMP compares the key to the value that was created on the previous startup, and if they do not match, BitLocker will lock the volume and prevent it from being accessed.

BitLocker can be configured to run on a system that does not support TMP, through the use of Group Policy. In this scenario the protection and encryption of the previously mentioned pre-execution files will not be available. When configured in this manner, encrypted keys can be stored on a USB Flash drive, and stored external to the specific hardware for protection.

BitLocker Drive Encryption can be disabled and re-enabled as required, in order to facilitate planned maintenance activities. It is not necessary to de-encrypt and re-encrypt volumes in order to enable or disable this function.

BitLocker Volume Recovery

In the event that something unforeseen should happen and a BitLocker protected file become unavailable to administrators with legitimate intent, there are recovery options that have been built in to this function, in order to allow those administrators to regain control over affected volumes.

There are three main levels of control over the security of the recovery information for BitLocker protected volumes:

- **Recovery Password.** The creation of a recovery password is a mandatory step in the process of enabling BitLocker Drive Encryption.
- **Active Directory** BitLocker can be configured to save recovery information directly to Active Directory, where it can be guaranteed to be always reliably available. This is the recommended solution for enterprise environments.
- **Group Policy Settings** Group Policy settings can be used to set mandatory requirements for the storage of BitLocker recovery information, and can also be used to prevent the enabling of BitLocker protection if those requirements have not been met.

BitLocker Management Options

Once implemented BitLocker Drive Encryption can be managed remotely by any of the following methods:

- **WMI (Windows Management Interface)** WMI can be used to control BitLocker settings throughout an enterprise in an efficient manner.

- **CLI (Command Line Interface)** The Command Line interface can be used to control BitLocker settings either locally or remotely. To manage BitLocker via the CLI execute the following script:
 - Manage-bde.wsf
- **BitLocker Remote Admin Tool** The BitLocker Remote Admin Tool can also be used to control BitLocker settings throughout an enterprise. The Remote Admin Tool must be installed by typing the following command at the command prompt:
 - ServerManagerCmd –Install RSAT-BitLocker

Using BitLocker for the Safe Decommissioning of Hardware

There are levels of protection that can be employed to protect BitLocker protected volumes from falling into the wrong hands, during transport, storage, or permanent decommissioning of hardware containing sensitive corporate data. The levels with increasing degrees of irrevocability are as follows:

- **Delete Keys from Volume Metadata** By deleting the keys from the volume metadata stored on the actual system, you remove the ability for anyone to access the files on the affected volume until administrators reintroduce a backed-up version of the needed keys to allow the volume to be decrypted and accessed once again. This option is most useful where hardware is intended to be stored in a non-secure location for an extended period of time, or when hardware will be transported from one location to another leaving it outside of the protection and influence of an organization's physical security for a period of time.
- **Delete Keys from Volume Metadata as Well as from all Backup Sources such as Active Directory, or USB Memory Keys** By deleting the keys not only from the volume metadata stored on the actual system, but also from all backup sources as well, you make the effects of BitLocker Volume Locking permanent. Nobody, including authorized administrators will be able to access the data on the subject hardware again.
- **Format Command** As an additional layer of protection the Format command has been written to specifically target sectors that could in any way be used to obtain access to the BitLocker encryption keys.

Data Collaboration

Windows Sharepoint Services is a feature that has come to be in great demand within organizations looking for effective ways to control and share knowledge and intellectual content amongst team members, as well as interdepartmentally. Sharepoint allows for intellectual resources to be shared via a Web interface in a way that is dynamic and highly controllable by administrators. Support for the underlying functionality of Sharepoint Services has been integrated into the Windows 2008 Server Operating System. Once all prerequisites roles and features have been installed the Sharepoint application can be installed to complete the requirements for the deployment of a Sharepoint server.

There are two levels of Sharepoint services that are available to be deployed on the Windows 2008 Server platform

- **Windows Sharepoint Services 3.0 SP1** Windows Sharepoint Services 3.0, or WSS 3.0 SP1 is designed to provide the base level of Sharepoint functionality. The features and functionality provided by WSS 3.0 are sufficient to satisfy the needs of most organizations looking to achieve a basic Sharepoint Services deployment.
- **Microsoft Office Sharepoint Services 2007** Microsoft Office Sharepoint Services 2007, or “MOSS 2007” is designed to provide a much more advanced level of functionality for organizations looking to achieve a more sophisticated level of Sharepoint Services deployment.



TEST DAY TIP

WSS 3.0 cannot be deployed on a Server Core installation of Windows 2008 Server, as many of the needed prerequisites are not available on a Server Core installation. WSS 3.0 deployment is therefore only supported on a Full Installation of Windows 2008 Server.

To successfully install WSS 3.0 on a Windows 2008 Server platform, there are a number of prerequisite Server Roles and features that must be installed in advance. Failure to satisfy all of these prerequisites before installing WSS 3.0 will result in an installation failure.

The needed prerequisite Server Roles are as follows:

- **Web Server Role** The Web Server Role is required to provide the needed IIS support for the Web-based interfaces utilized by Sharepoint Services.

TEST DAY TIP

The **Application Development | .NET Extensibility** must also be manually selected during Web Server Role installation in order to support the deployment of WSS 3.0. This component can be selected during the installation of the Web Services Role, when the **Role Services** page is presented. Failure to add this required component will result in a failure of the installation of the actual WSS 3.0 instance. You will however be prompted to add this component at a later point, during the installation of the .NET Framework 3.0 Feature set, which we'll mention shortly.

TEST DAY TIP

The **IIS 6.0 Management Compatibility Component** must be manually selected over and above the default components of the Web Services Role in order to support a deployment of WSS 3.0 AP1. This component and all of its subordinate dependant components can be selected during the installation of the Web Services Role, when the Role Services page is presented. Failure to add this required component will result in a failure of the installation of the actual WSS 3.0 instance. You will not be prompted for the addition of this Role Service, so it is important not to forget to add it during Web Service Role installation

- **The Windows Process Activation Service (WPAS)** The Windows Process Activation Service provides functionality which is designed to remove the dependency on the HTTP protocol.
- **The Process Model** The Process Model subcomponent is used to support Web and WCF Services.
- **The Configuration API** The Configuration API subcomponent provides support for other programs that have been written to take advantage of this method of Web interface.
- **The .NET Environment** The .NET Environment subcomponent is required to support the underlying functionality of WSS 3.0 SP Service.

NOTE

You will be automatically prompted to add the Windows Process Activation Service as well as its subordinate components during the Web Services Role installation process.

However, you will not be automatically prompted to add the **WPAS .NET Environment** subcomponent during the installation of the Web Services Role. This is because the first two subcomponents, Process Model and Configuration API, are known dependencies for the Web Services Role and are therefore picked up as needed subcomponents during its install. The .NET Environment subcomponent of the Windows Process Activation Service is a more specific requirement needed for the WSS 3.0 SP1 deployment. Since you are not installing the WSS 3.0 software at this point, the association to this dependency is not made. You will however be prompted to add this component at a later point, during the installation of the .NET Framework 3.0 Feature set, which we'll mention shortly.

The needed prerequisite server features are as follows:

- **.NET Framework 3.0** The .NET Framework 3.0 Feature is a necessary supporting component that can be added through the Add Features Wizard found in the Server Manager Console Web Server Role, and is required to provide the needed IIS support for the Web based interfaces utilized by Sharepoint Services.

NOTE

At the point where the **.NET Framework 3.0 Feature** is selected for installation, you will be automatically prompted to add the **Application Development | .NET Extensibility**, and the **Windows Process Activation Service | .NET Environment** Role Services subcomponents if they were not added previously during the Web Service Role installation process.

At this point, you are ready to install WSS 3.0 SP1. It is downloadable and comes in the form of a single executable file. Run the executable to proceed with the installation of WSS 3.0 SP1.

Once executed, you will be presented with the following installation options:

- **Basic** Install Single Server Standalone using default options.
- **Advanced** Choose settings for Single Server or Sharepoint Server Farm.

The selection chosen at this point obviously depends on what sort of architecture and level of organization your company wishes to apply to its Sharepoint deployment.

NOTE

The deployment of the **WSS 3.0 Server Role** is an exception to the normal Windows 2008 Server method of Role deployment where such items are simply selected under the **Add Roles Wizard** and installed on an as-desired basis. Microsoft has stated that it intends to maintain the deployment of the **WSS 3.0 Role** in this format for the foreseeable future.

NOTE

During the installation of WSS 3.0 AP1 you will be prompted to take note of the fact that the IIS service, as well as the Sharepoint services, will be stopped. This is designed to warn you that there will be interruptions to other Web sites if any are running on the subject server.

Head of the Class...

Sharepoint Farms

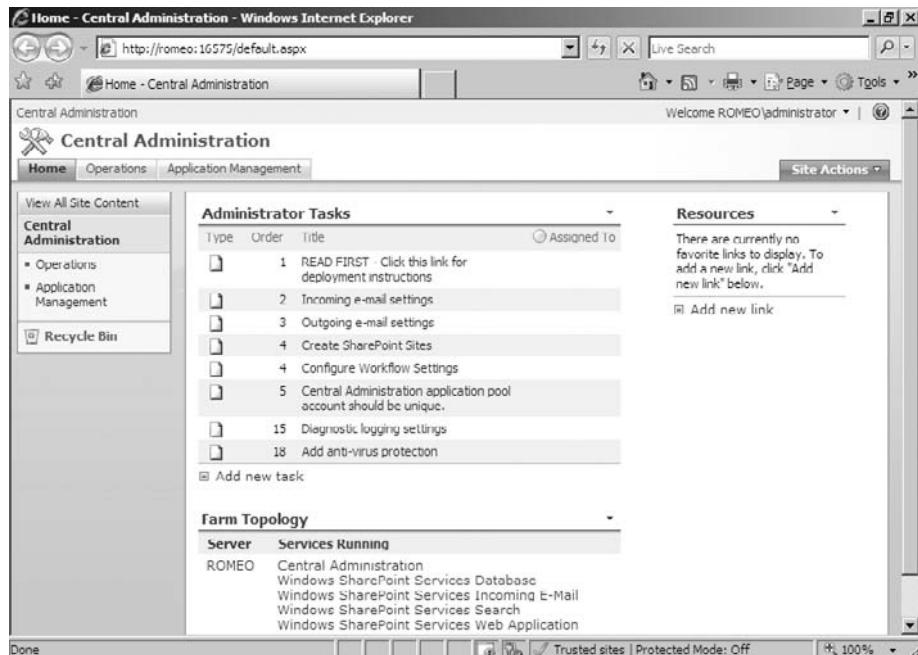
A very common scenario that I have seen develop within larger organizations is the rush for each individual department to develop and deploy their own individual Sharepoint solutions, with little to no planning or thought applied to the overall Sharepoint requirements of the organization as a whole. This is a problem that can easily and quickly grow out of control, until one day managers realize that they may have 50 separate instances of Sharepoint running, all very inefficiently using company resources such as data center space, with its associated power, cooling costs, etc., not to

Continued

mention the administrative time and effort that goes into the creation and support of each of these autonomous instances. A bit of forward thinking and planning applied to this situation in advance of such Sharepoint sprawl can result in the creation of an organized Sharepoint farm that will satisfy the needs of all parts of an organization, while minimizing the waste of administrative effort and physical resources that inevitably result from the previously mentioned situation. I've seen this happen quite frequently, and in fact was approached just last week by someone from a specific department who was asked to deploy a Sharepoint instance specifically for the benefit of that department. He was astute enough to notice that the rampant deployment of Sharepoint Web sites within that company was a problem that was turning into a growing monster, and he was asking about options to amalgamate these individual instances into an organized farm. Of course, I told him that this was possible, although much more administratively costly and time-consuming when planned and executed after the fact.

Figure 9.4 is an example of the Windows SharePoint Services 3.0 SP1 central administration Web site.

Figure 9.4 Windows SharePoint Services 3.0 SP1 Central Administration Web Site



Planning for High Availability

High Availability is a term that can be applied to a wide range of solutions from Server Clustering all the way down to server hardware-based RAID solutions and redundant power supplies. Ultimately this term can accurately be described as any solution where measures have been taken to decrease the level of vulnerability of a service or resource to interruptions in availability caused by unforeseen failures or events. These efforts to create redundancy could be for an application or data upon which users depend, or for the underlying hardware or infrastructure that said applications or data run on. In this section we will look at some of the new features and improved functions offered with Windows 2008 server that are designed to meet the needs of customers looking to achieve high availability for their most important IT resources.

Two main solutions offered by Microsoft are designed to meet the needs of those looking to achieve highly available solutions for their critical services. They are as follows:

- **Failover Clustering** Failover Clustering is the solution most commonly applied for applications such as SQL and Exchange that are considered critical to business activity, and therefore intolerant to downtime. The use of clustering allows for activities such as planned maintenance to the O/S to be carried out without interruption to the application layer running on the platform. As well, unanticipated hardware failures or other such similar events affecting any one of the Clustered Nodes will not result in any interruption of service to the dependant application
- **Network Load Balancing** Network Load Balancing is the solution most commonly applied to applications such as Web servers, where an array of servers can be configured to equally share the load of incoming client requests in a dynamically balanced manor. As with Failover Clustering the loss of any one individual host in the array will not result in the loss of the availability of the overall application. One major difference however is that unlike with clustering solutions where the failure of an individual node does not result in any interruption of service to connected clients, all client connections to the failed host in a Load Balancing scenario will be lost.

Failover Clustering

Failover Clustering has been dramatically improved in Windows 2008, and many of the common points of dissatisfaction with previous iterations of failover clustering

have been addressed. Many of the new features and functionalities offered with Windows 2008 clustering have been targeted at the following areas:

- **Simplification** There has been an effort with this newest version of clustering to simplify not only the initial setup and configuration process for clustering, but also the ongoing administration of running clusters. Previous versions of Windows Clustering have been accused of being overly complicated to understand, and therefore difficult to properly deploy. Microsoft has made a concerted effort to remove this limitation in Windows 2008.
- **Improved Stability** There have been significant improvements included in this latest version that have been designed to deal with the well-known cluster stability and recoverability problems that were associated with previous versions.
- **Improved Security** As with all aspects of the new Windows 2008 operating system security is an ever-present factor in many of the features and functions—something that has been made necessary by the realities of the wide spread-proliferation of hackers and malicious code that are omnipresent in the modern world of IT. .

Architectural Details of Windows 2008 Failover Clustering

One of the most notable improvements to Failover Clustering functionality in Windows 2008 is the redesigned capabilities and functionality of the Quorum, now called the **Witness Disk**. The Witness Disk can now be configured in a manner that will allow the cluster to survive its loss in the event of a failure. As well, the options offered for the configuration and placement of the Witness Disk mean that Failover Clustering can be configured with a level of flexibility that has never before been possible for Clustered Solutions. The Witness Disk is no longer limited to SAN type directly attached physical storage. It can be configured to reside on a file share anywhere in the organization. In fact a dedicated file server could be configured to host many Witness Disks for many different Clusters. While this capability does exist it might be considered prudent not to do this, in order to avoid creating a single point of failure for multiple Clusters, something that is obviously contrary to the entire purpose of deploying a Failover Clustering Solution in the first place. One option that is viable, however, is to create such a Witness Disk hosting type of

dedicated File Server on a Clustered File Server, in order to improve the availability and reliability of this solution. Once again, while this is an available option, the implementation of a Failover Clustering solution in this configuration is something that should be carefully thought out in advance, to ensure that all factors have been effectively considered, before putting all the eggs in one basket so to speak.

In Windows 2008 the most desirable features and functions of previous Quorum models have been combined to create the **Majority Quorum Model**. In the Majority Quorum Model a vote system has been implemented, in order to assign a value to each copy of the cluster registry files. Specifically, each node and the Witness disk itself are assigned one vote, and as long as the majority of votes are online and available, so will the cluster. The way this works is that the disk on each node of the cluster that runs a copy of the key quorum registry files gets a vote. As well, the Quorum itself gets a vote since it is also obviously supporting a copy of these same key files. As long as the majority of votes are online and available, then the cluster will continue to run. This is made possible by the fact that a copy of the Quorum or Witness Disk contents are maintained on the local drives of each Node, as well as on the Witness Disk itself. Therefore losing a node or losing the Witness Disk are effectively the same. It's just one copy out of three available copies that will have been lost. The two copies that remain online and available represent the Majority of the available copies.

The **Majority Quorum Model** can be deployed according to any of the following configurations:

- **Votes for Each Node and the Witness Disk** With votes assigned to each Node as well as the Witness Disk, the Cluster can survive the loss of any one of these resources.
- **Votes for Each Node Only** This will behave the same as the Shared Quorum Model employed in Windows 2003 Clustering. The Cluster will continue to function as long as the Witness Disk and one of the Nodes of the Cluster remain online. This configuration will not survive the loss of the Witness Disk.

Failover Clustering is an optional feature in Windows 2008 Server that must be installed before a server can be deployed as a node in a cluster. The Failover Clustering Feature is also a required component in order to make the Failover Clusters Manager Tool available under Administrative Tools. To install the Failover Clustering Feature select **Start | Administrative Tools | Features | Add Features**.

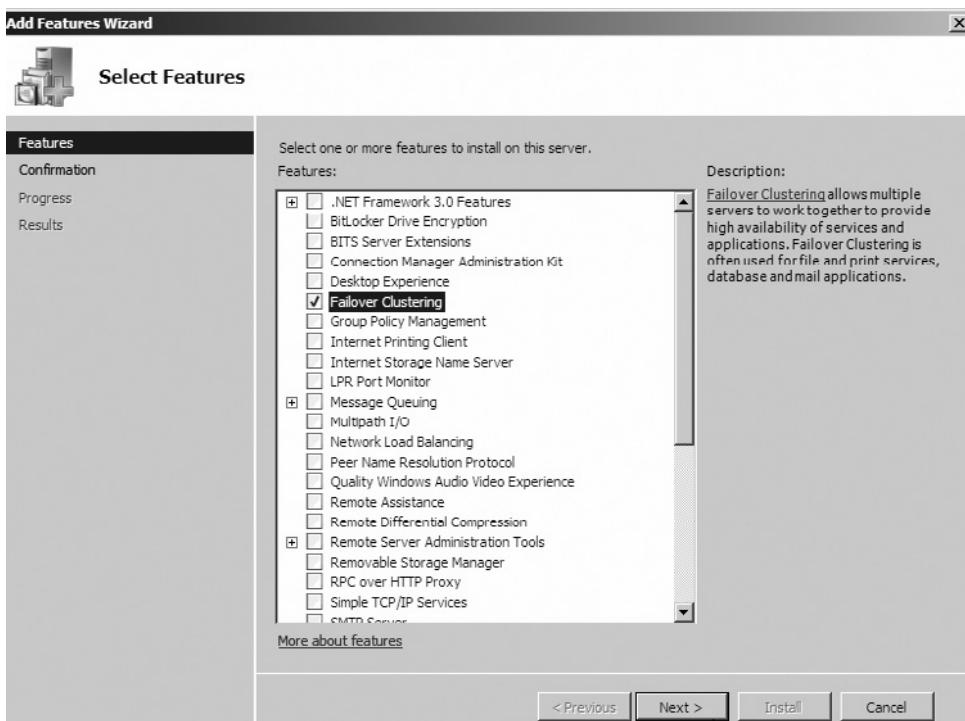
EXERCISE 9.1

INSTALLING THE FAILOVER CLUSTERING FEATURE ON A FULL INSTALLATION OF WINDOWS 2008 SERVER

As a prerequisite this exercise assumes the pre-existence of a full installation of Windows 2008 Server that has been fully configured with all supporting requirements in place. The *Add Features* procedure for the addition of the Failover Clustering Feature needs to be performed on each server that is intended to be a node in the cluster being configured.

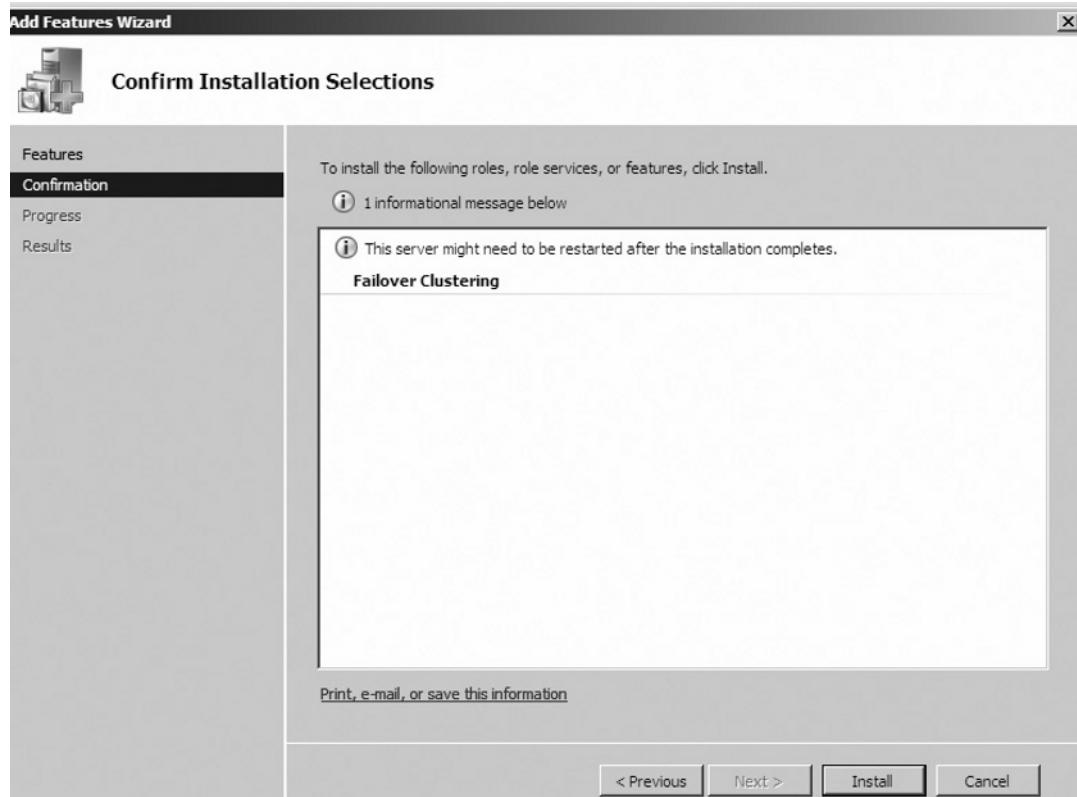
1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Features | Add Features**.
3. Select **Failover Clustering Feature** and then click **Next** to proceed (see Figure 9.5).

Figure 9.5 Add Features Wizard “Select Features” Screen

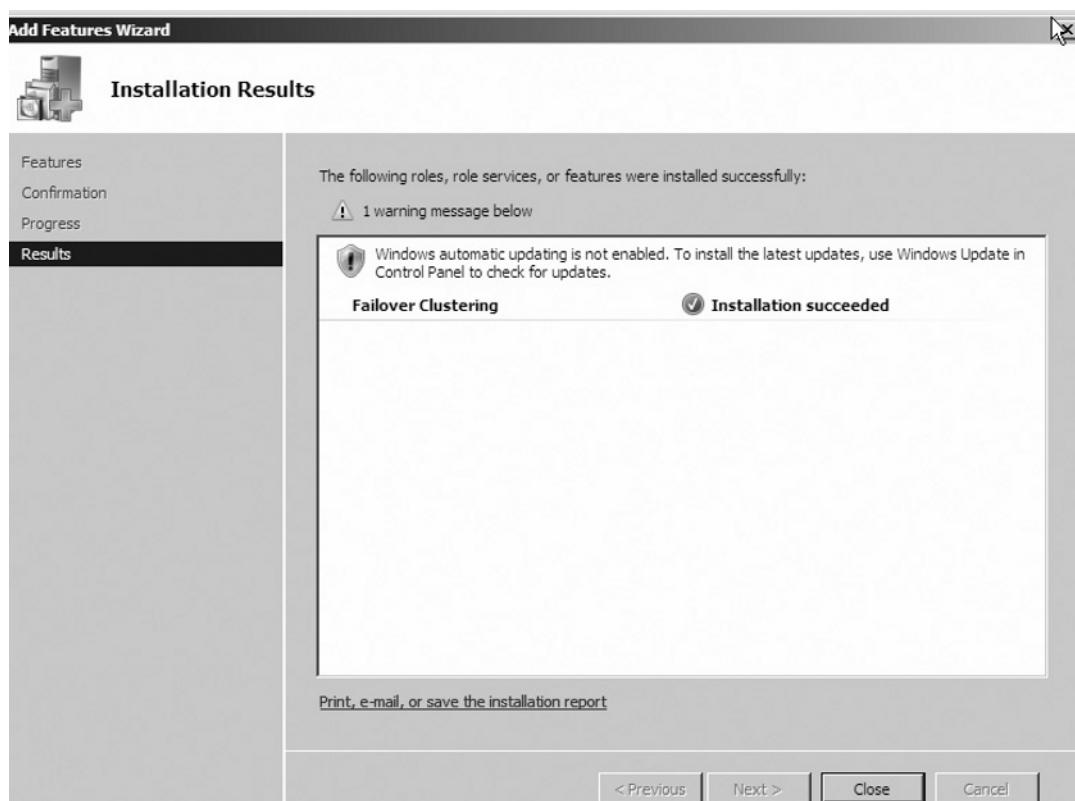


4. When the **Confirm Installation Selections** page appears, click **Install** to proceed (see Figure 9.6).

Figure 9.6 Add Features Wizard “Confirm Installation Selections” Screen

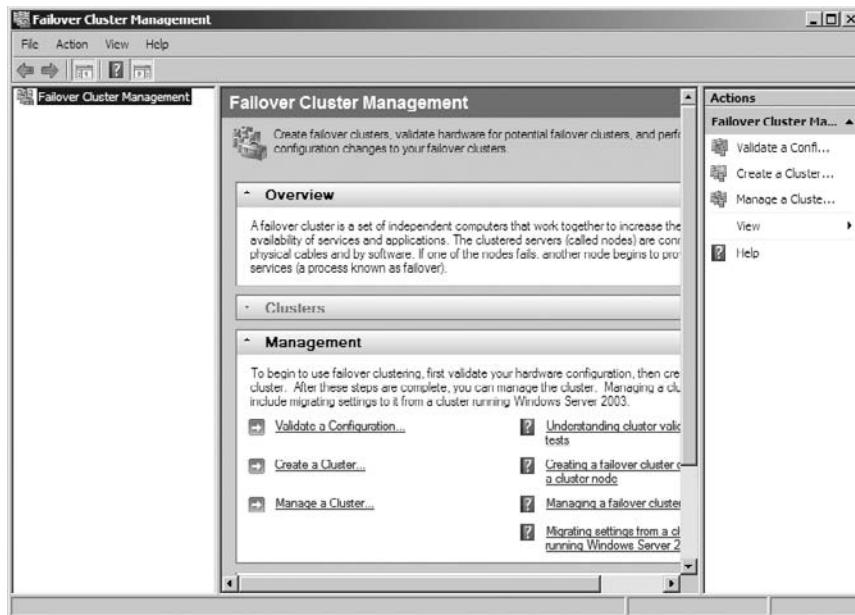


5. Once the installation is finished select, click **Close** to finish the wizard, as seen in Figure 9.7.

Figure 9.7 Add Features Wizard “Installation Results” Screen

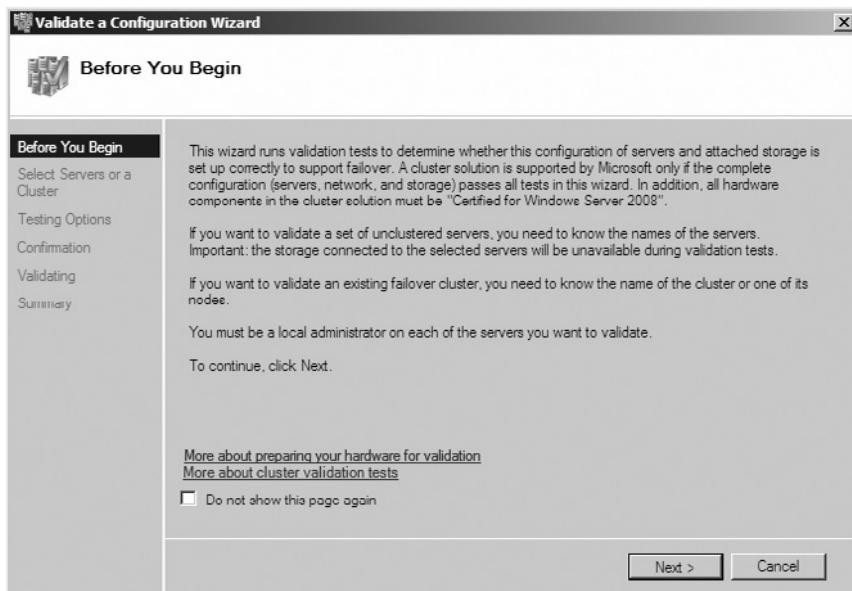
6. Select **Start | Administrative Tools | Failover Cluster Manager**.
7. In the Actions Pane in the upper right, select **Validate a Configuration** (see Figure 9.8).

Figure 9.8 Failover Cluster Management Console—Prior to New Cluster Creation



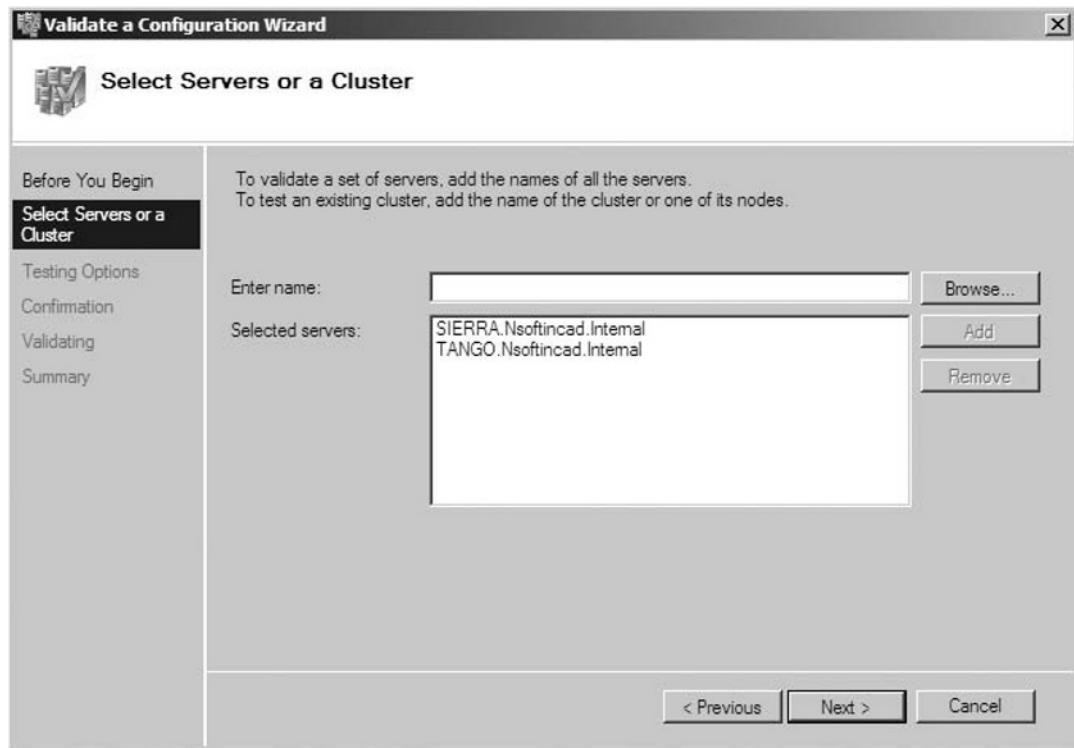
8. Read the information provided on this page, and then select **Next** to continue (see Figure 9.9).

Figure 9.9 Validate a Configuration Wizard—“Before You Begin” Page



9. On the **Select Servers or a Cluster** page enter the names of the servers intended to be nodes in the cluster to be created (see Figure 9.10).

Figure 9.10 Validate a Configuration Wizard—“Select Servers or a Cluster” Page



TEST DAY TIP

If the installation of the Failover Cluster Feature has not been completed on each of the subject servers, they will report as being *Unreachable*.

NOTE

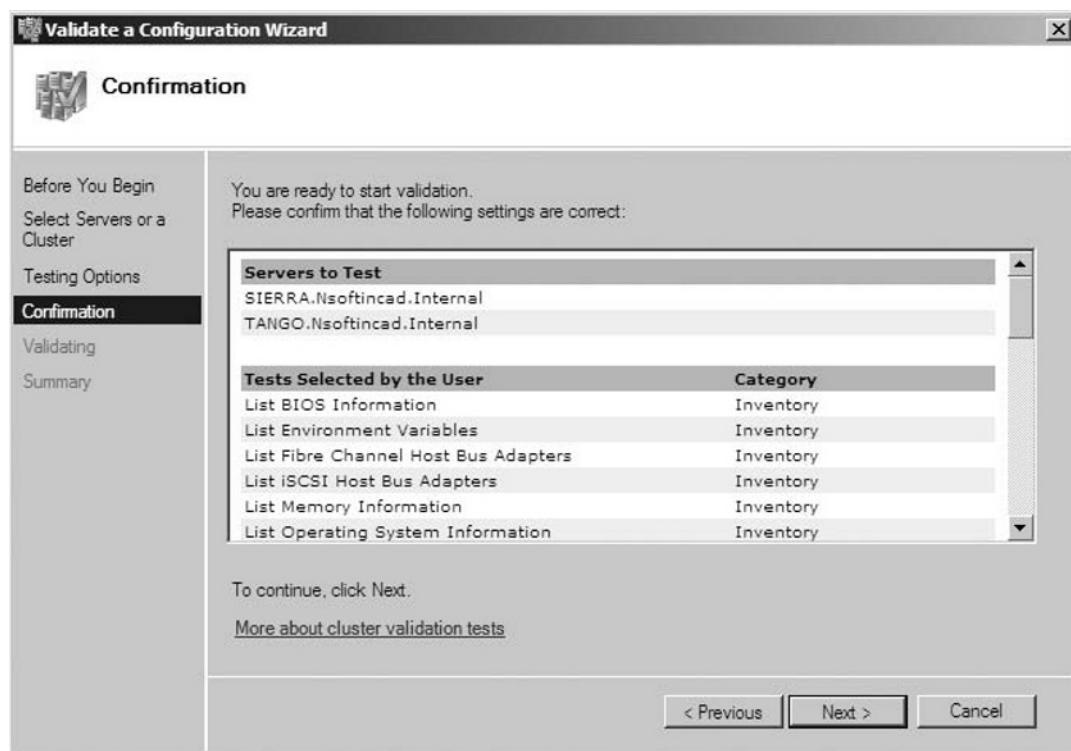
If Windows Firewall Protection is configured to block Remote Procedure Calls on the target node servers this will also cause them to report as being *Unreachable*.

10. Select the **Run all Tests (recommended)** option and then click **Next** to proceed (see Figure 9.11).

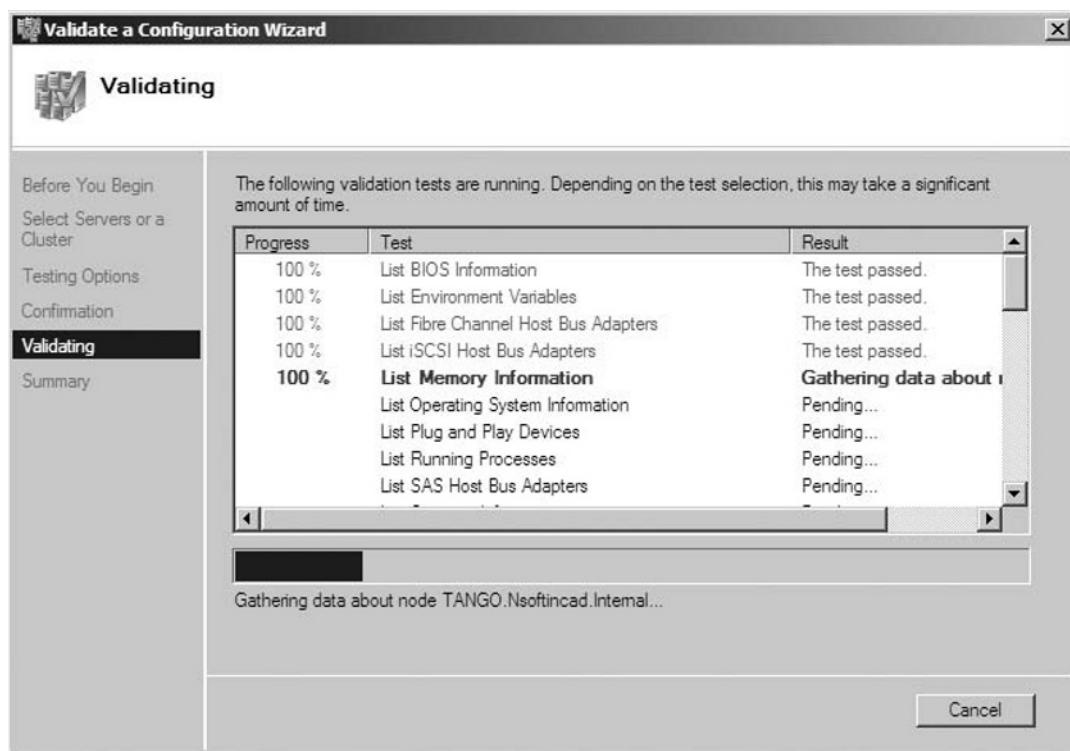
Figure 9.11 Validate a Configuration Wizard—“Testing Options” Page



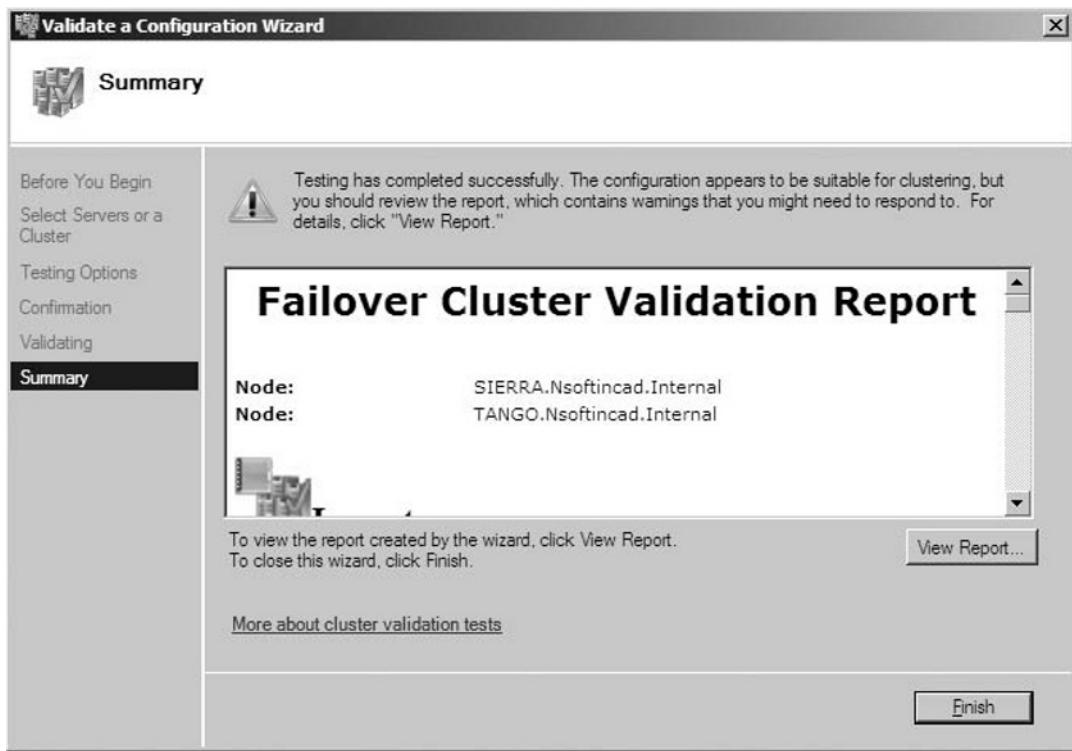
11. After confirming the selected options (see Figure 9.12), click **Next** to proceed.

Figure 9.12 Validate a Configuration Wizard—“Confirmation” Page

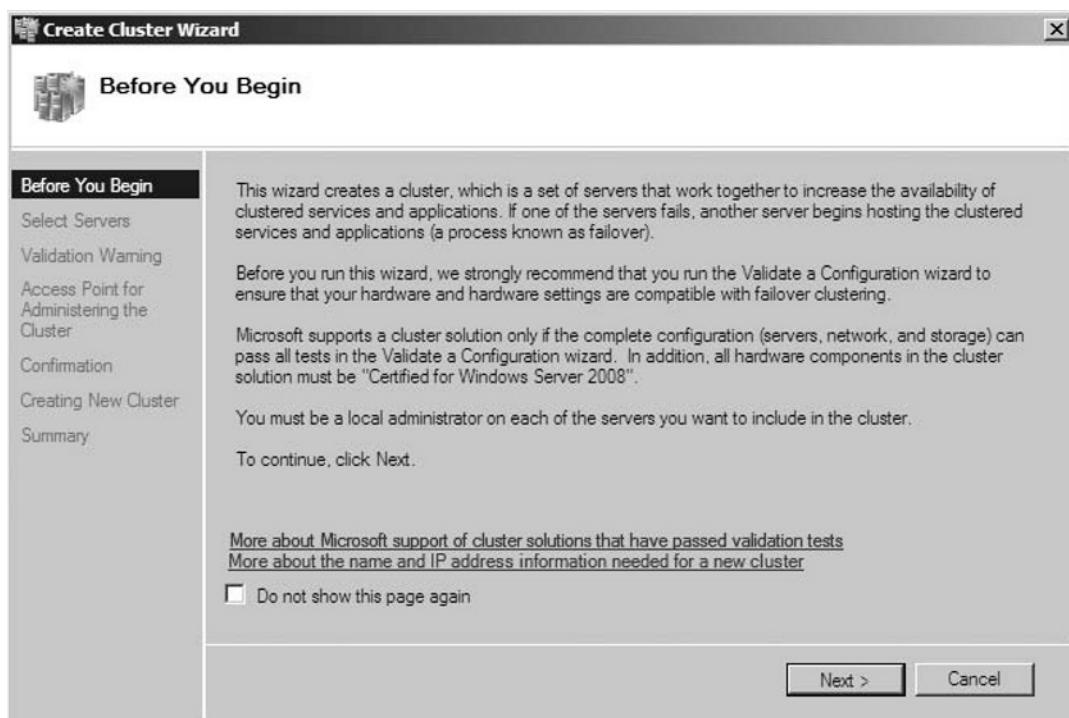
12. It will take a few minutes for the Validation process to run, as shown in Figure 9.13.

Figure 9.13 Validate a Configuration Wizard—“Validating” Page

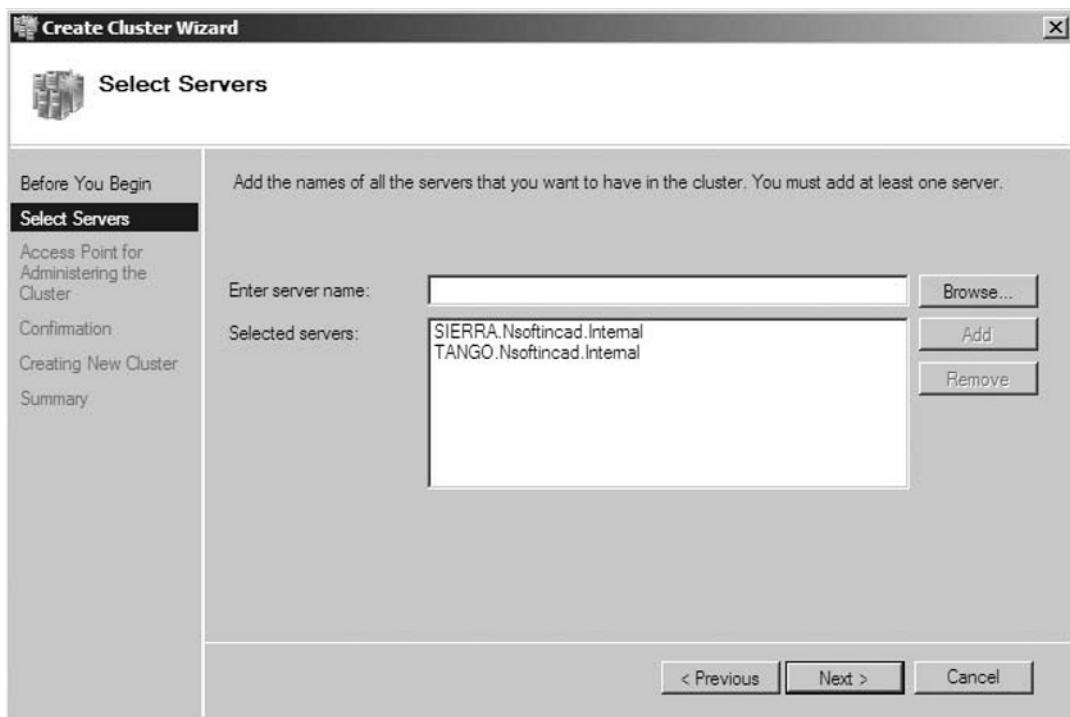
13. Once completed, review the generated **Failover Cluster Validation Report**.
14. Resolve any issues identified in the report, prior to proceeding to the Cluster Creation process in the next step (see Figure 9.14).

Figure 9.14 Validate a Configuration Wizard—“Validation Summary” Page

15. Once all issues identified in the **Failover Cluster Validation Report** have been resolved, proceed to open the **Failover Cluster Management Console**.
16. Under the Actions Pane in the upper right hand select **Create a Cluster**.
17. On the Create Cluster Wizard **Before You Begin** page, review the information presented, and then select **Next** to proceed (see Figure 9.15)

Figure 9.15 Create Cluster Wizard—“Before You Begin” Page

18. Just as was done with the Cluster Validation Wizard, when the **Select Servers** page displays, enter the names of the servers intended to be Nodes in the new Cluster (see Figure 9.16).
19. Select **Next** to proceed.

Figure 9.16 Create Cluster Wizard—“Select Servers” Page

TEST DAY TIP

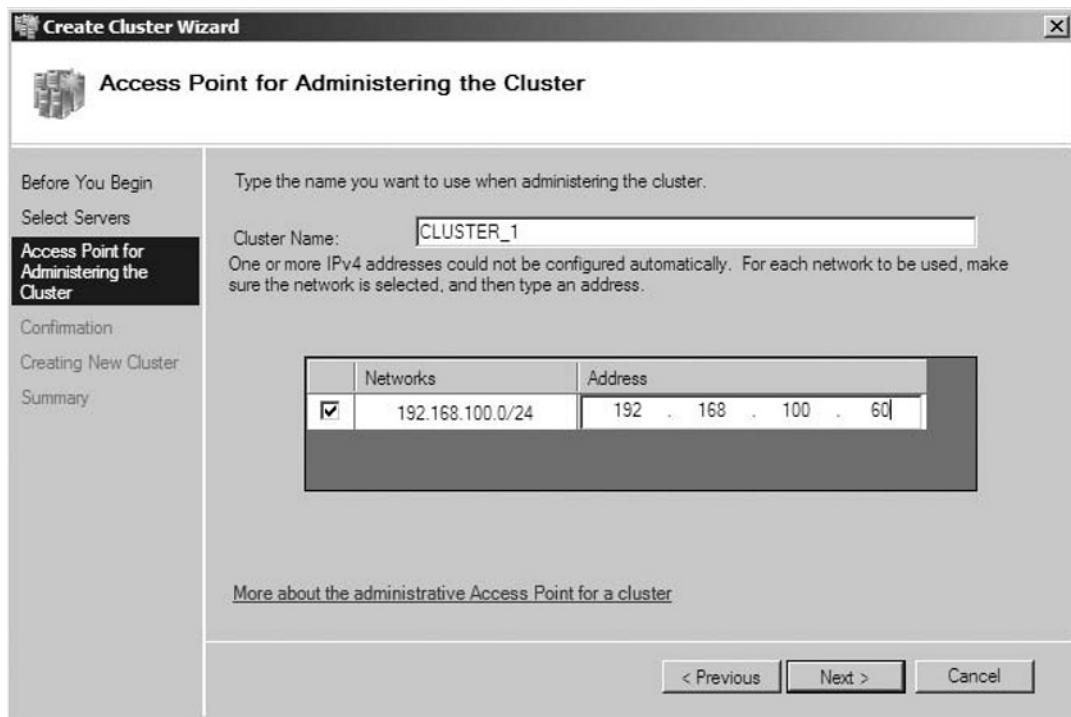
If the installation of the **Failover Cluster Feature** has not been completed on each of the subject servers, they will report as being *Unreachable*.

NOTE

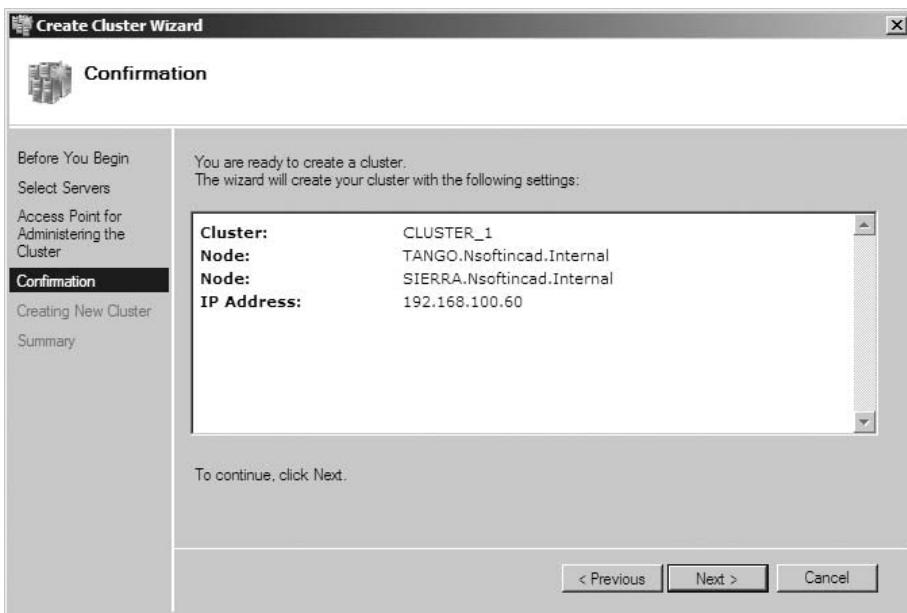
If Windows Firewall Protection is configured to block Remote Procedure Calls on the target node servers, this will also cause them to report as being *Unreachable*.

20. On the **Access Point for Administering Cluster** page, enter the **Cluster Name** that will be used to access and refer to it, as well as the **IP Address** that will be associated with this Cluster name.
21. Select **Next** to proceed, as shown in Figure 9.17.

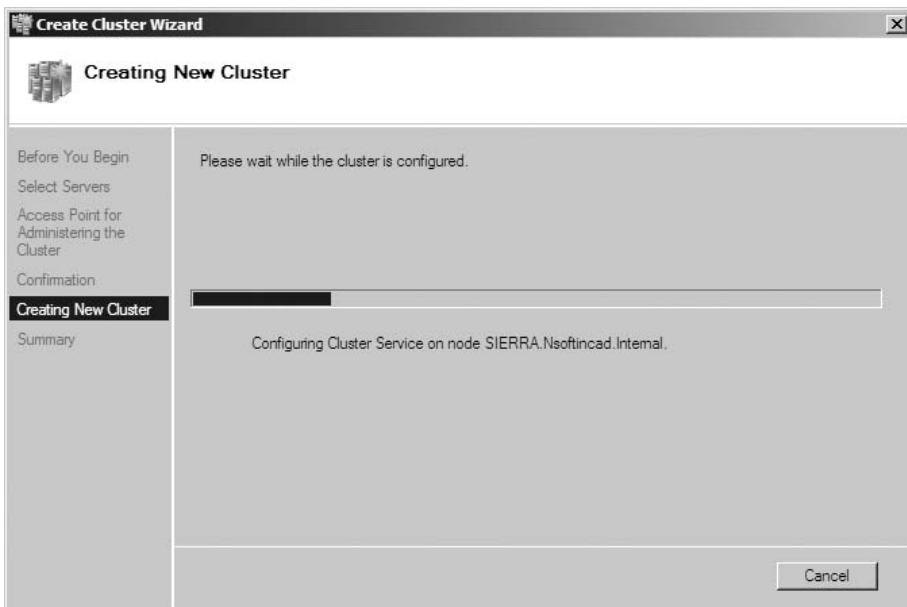
Figure 9.17 Create Cluster Wizard—“Access Point for Administering the Cluster”



22. On the **Confirmation** page confirm all Cluster Creation Selections.
23. Select **Next** to proceed (see Figure 9.18).

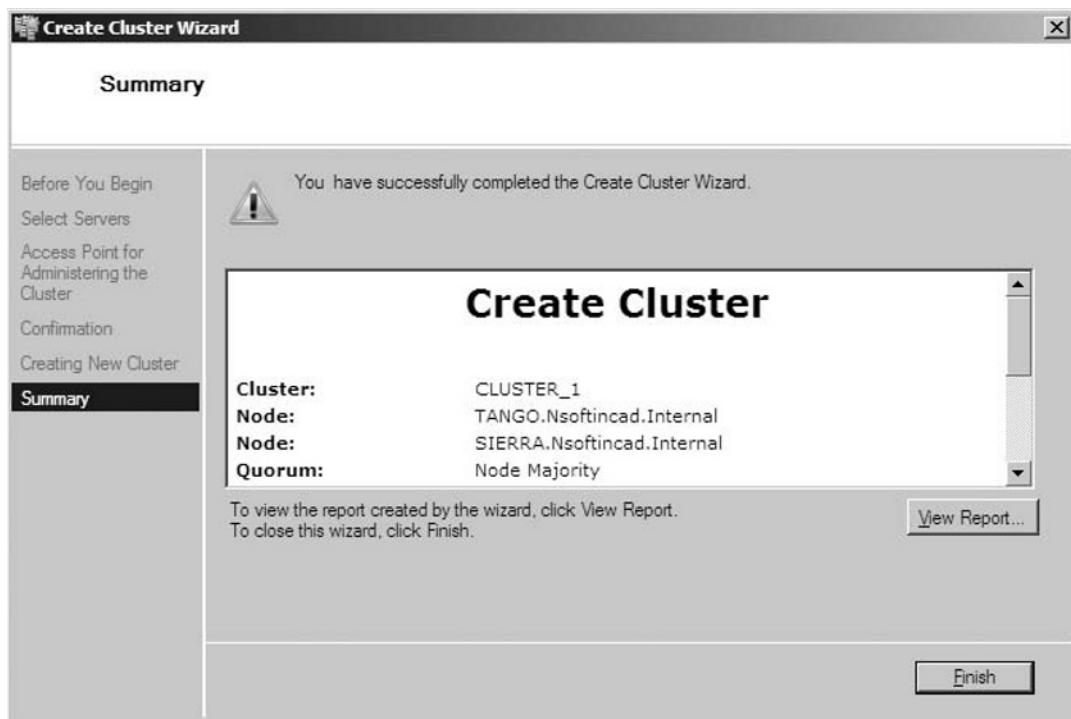
Figure 9.18 Create Cluster Wizard—“Confirmation” Page

24. The **Creating New Cluster** process will take a few minutes to run (see Figure 9.19).

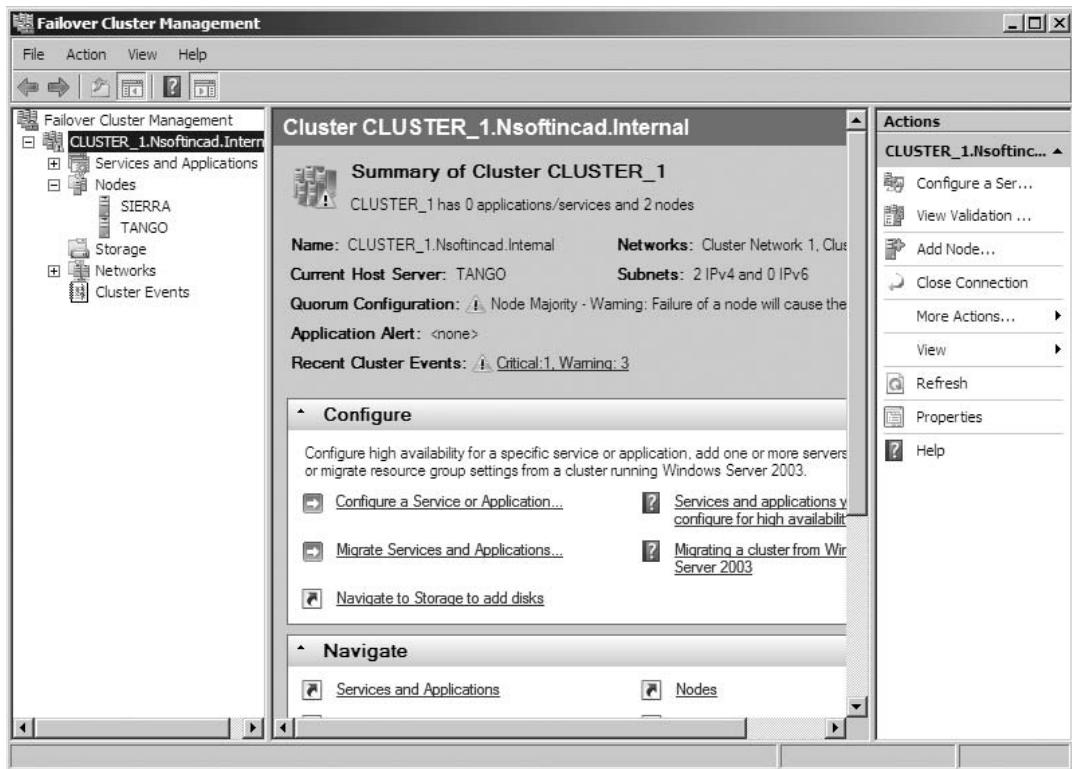
Figure 9.19 Create Cluster Wizard—“Creating New Cluster” Page

25. Once completed, review the **Create Cluster Summary Report** to ensure that all Cluster Creation processes ran successfully, and provided the desired result.
26. Once the report has been reviewed, and everything has been verified, select **Close** to complete the Cluster creation process, as shown in Figure 9.20.

Figure 9.20 Create Cluster Wizard—“Summary” Page



27. Select **Start | Administrative Tools | Failover Cluster Manager** to view the details of the newly created Cluster (see Figure 9.21).

Figure 9.21 Failover Cluster Management Console

28. The New Cluster Creation Process has now been successfully completed.

Multi-Site Clusters

The ability to support multi-site clustering was available with Windows 2003 Server; however, the requirement that each node of the cluster be on the same subnet meant that VLANs had to be used to trick the cluster into believing that the nodes were actually on the same subnet. As well, limitations with the amount of delay that the heartbeat could tolerate without misreading the situation as a failed host meant that nodes could not be placed very far apart, and not without a high speed connection between them.

Windows 2008 Server's version of Failover Clustering has overcome these issues by implementing the following key changes to cluster architecture:

- **Heartbeat—Configurable Delay** In Windows 2003 Server the maximum delay that the heartbeat would tolerate before detecting a node failure was 500 milliseconds. By making the heartbeat delay wait time configurable to essentially any value in Windows 2008 Server, the limitation on distance and connection speed between cluster nodes has been effectively eliminated. This means that cluster nodes can reside in different cities, or even different countries, without issue. This is a feature that has significant implications for any organization's Disaster Recovery Solutions, as the capability to deploy geographically dispersed cluster nodes means that there is a significant reduction in the susceptibility to issues such as large scale power outages and so forth. Even if an entire city were to be affected by such an event, an alternate cluster node running in a different city could still provide failover capability, ensuring that the critical applications running on it would remain available throughout the duration of the event.
- **Subnet Flexibility** In Windows 2008 Failover Clustering the nodes can be configured to exist on different subnets. This feature is designed to support the ability to have geographically displaced nodes without the need to use VLANs as was the case with Windows Server 2003 Clustering. With Windows 2003 the individual Cluster Nodes were required to be running on the same subnet in order for the cluster to function. This necessitated the use of Virtual Local Area Networks (VLANs) at the network level in order to trick the cluster into believing that the different nodes running at separate physical locations with different subnets were actually running on a common subnet. This added level of configuration complexity often discouraged the use of this technology, due to fears of potential troubleshooting difficulties with any cluster connectivity or failover issues. The removal of this limitation in Windows Server 2008 Failover Clustering will make the implementation of geographically dispersed cluster solutions a much more attractive and viable option for a wide range of differing requirements.

This greatly improved support for the implementation of geographically dispersed clustering implementations is something that I'm sure many organizations will be taking a serious look at. The implications for cheaper and easier-to-implement Disaster Recovery solutions are obvious.

Service Redundancy

The ever-increasing demand in organizations for Service Redundancy has been addressed in Windows 2008 server in a number of ways. The most notable

to me is the feature set offered to address the need for Service Redundancy at the Application level. The features in question are most notably applied to Exchange Server 2007 Clustering solutions, in order to provide not just a High Availability, but also Service redundancy for the critical Exchange service. This solution uses a highly customized form of replication technology to ensure that all components of the Exchange Service are fully redundant, and always available regardless of what happens. This solution can be deployed in any of the following configurations:

- **Cluster Continuous Replication (CCR)** The Cluster Continuous Replication (CCR) solution provides the highest level of service and data redundancy. It accomplishes this by allowing for the replacement of the shared storage model used by traditional cluster configurations, and replacing it with a storage group model. In the Storage Group Model the required common storage is maintained on a separate server, or servers. In this scenario the data contained on multiple storage group members is kept in constant synchronization. When applied to a disaster recovery scenario this configuration would allow for instant failover to a fully up-to-date version of production data, with no loss of service to end users.
- **Standby Continuous Replication (SCR) Introduced as a new feature with the release of Exchange 2007 SP1** Standby Continuous Replication is designed to be deployed using an Active / Passive sort of model, where the secondary application servers are kept up to date, but not to the moment. With this solution, there may be a small amount of interruption to service availability, as well as potential transactional data loss; however, the amount of network-based replication traffic, and the resulting lower cost of implementation, would be acceptable for some organizations who can tolerate these factors. SCR is only available in Exchange Server 2007 SP1 (or later).
- **Single Copy Clusters (SCC)** The Single Copy Cluster configuration model is the standard configuration for a traditional Failover Clustering solution. As the name implies, in this configuration, only one copy of the relevant data is maintained on a common storage location. While this does provide High Availability capabilities, it does not by itself offer the Service and Data redundancy provided by the first two solutions. It is important to note, however, that this solution can be combined with CCR and SCR solutions in a flexible manner in order to provide any desired data and service redundancy capabilities.

Service Availability

In Windows Server 2008 the greatly simplified ability to cluster core network infrastructure resources has provided an easy way to ensure that key infrastructure components, upon which an organization depends, will always be available and online. The following key infrastructure resources are available options to be clustered through the use of the High Availability Wizard found in the Failover Cluster Management Console.

- **DFS Distributed File System** Distributed File System provides redundancy and replication capabilities across multiple servers and/or locations for critical company data. To further increase the level of availability for any data that is being provided in this manner, a clustered solution can be deployed to guarantee its availability regardless of what might happen.
- **DHCP Dynamic Host Configuration Protocol** Dynamic Host Configuration Protocol is another service on which most organizations depend heavily. If it were ever to go down for any reason, the potential financial impact of all work stations users not being able to access the network would be substantial to say the least. For this reason, DHCP has also been included as a clusterable resource in Windows 2008 Server.
- **DTC Distributed Transaction Coordinator Service** The Distributed Transaction Coordinator Service can be just as critical as those previously mentioned in any organization, and has thus also been included as a clusterable resource under Windows 2008.
- **Print Services** Print Services is a service whose importance is often taken for granted in any modern organization. It can often be viewed as a service of lesser importance by administrators, until of course it becomes unavailable. It's often only then when the entire organization begins complaining simultaneously that its criticality to daily business operations is realized. To assist in the avoidance of such a scenario, the ability to create highly available print services has been integrated into the Windows 2008 High Availability Management package.

Data Accessibility and Redundancy

There are two main solutions offered with Windows 2008 server that are designed to provide highly available accessibility and redundancy for an organization's critical data resources. They are Distributed File Services and Failover Clustering.

Failover Clustering

The addition of the File Server Role to Windows 2008 Server, as well as the improved ability to create a file server solution on a clustered platform, has made it significantly easier to deploy and manage highly available solutions for your organization's critical data resources.

Prerequisites

To create a highly available file server solution in Windows 2008, the following prerequisites must be met:

- **File Server Role** The File Server Role is an optional add-on Role in Windows Server 2008. It must be installed via any of the previously discussed methods, prior to any attempt to create a highly available File Server Solution. Each server that is intended to be deployed as a node in the File Services Cluster to be created must have this Role installed.
- **Storage Components adequate to support a Server 2008 based Failover Cluster** Shared storage components as required to support the deployment of a Failover Cluster based on a minimum of 2 nodes running the Windows 2008 Enterprise O/S must be in place, and fully operational, prior to any attempt to create a highly available File Server Solution.
- **Validate Cluster Configuration** Prior to the creation of the File Server Failover Cluster, open Failover Clustering Management Console, and run the Validation Wizard to ensure that all required components are not only in place and available, but running in a configuration that will adequately support the creation of a Failover Cluster.

EXERCISE 9.2

CREATING A FILE SERVICES CLUSTER

As a prerequisite this exercise assumes the pre-existence of a full installation of Windows 2008 Server that has been fully configured with all supporting requirements in place.

1. Select Start | Administrative Tools | Failover Cluster Manager and in the upper right-hand corner under the Actions Pane, select **Configure a Service or Application**.
2. On the **Select Service or Application** screen select **File Server** and then click **Next**.

3. On the **Client Access Point** screen provide a **Cluster Name** and **IP Address** to be used for connection to, and management of, the new cluster. Once done, select **Next**.
 4. On the **Select Disks** screen choose the “**Shared Disks**” where the highly available data will be stored. Once done, select **Next**.
 5. On the **Confirmation** screen confirm all selections, and select **Next** to proceed.
 6. Once the Creation process is complete select **Close** to finish.
 7. Select **Start | Administrative Tools | Failover Cluster Manager** and view and manage the newly created file service.
-

New & Noteworthy...

Failover Clustering File Services

New to Windows 2008, Failover Clustering File Services is the ability to create file shares on a File Services Cluster using Windows Explorer.

Distributed File System

Distributed File System can be a very effective way not only to provide data redundancy, but also greatly enhanced accessibility for client users that are geographically dispersed from the main infrastructure resources of an organization. Through the use of DFS Replication, updates made to corporate data can be automatically replicated to DFS member servers at remote locations, allowing the user at these locations to access “always up to date” information hosted from a central location, yet with local access speeds and quality of connection. For many national or international level organizations, this functionality can be a business critical core capability, without which the company could not function effectively.

As mentioned previously, this critical service can be clustered in a high availability solution in order to ensure uninterrupted access to DFS based data at all times, for those that depend upon it.



TEST DAY TIP

DFS Services can be deployed on either a Server Core or a Full Installation of Windows 2008 Server.

The DFS service is an optional component in Windows 2008 that is meant to be used together with the File Service Role. DFS Services itself is also supported by the following subordinate services:

- **DFS Namespace Service** The DFS Namespace Service is used to organize the DFS links to data from multiple file servers into one common interface for easy access by end users.
- **DFS Replication Service** The DFS Replication Service provides the replication functionality necessary to maintain multiple copies of DFS-based data hosted in multiple locations in a consistent single version state.
- **Windows Server 2003 File Services** This optional service supports DFS replication with 2003-based legacy DFS systems.

Unless manually deselected, these first two subordinate services will be automatically selected and installed along with the DFS Service, when it is selected for installation. The third, Windows Server 2003 File Services, will only be installed if manually added when required.

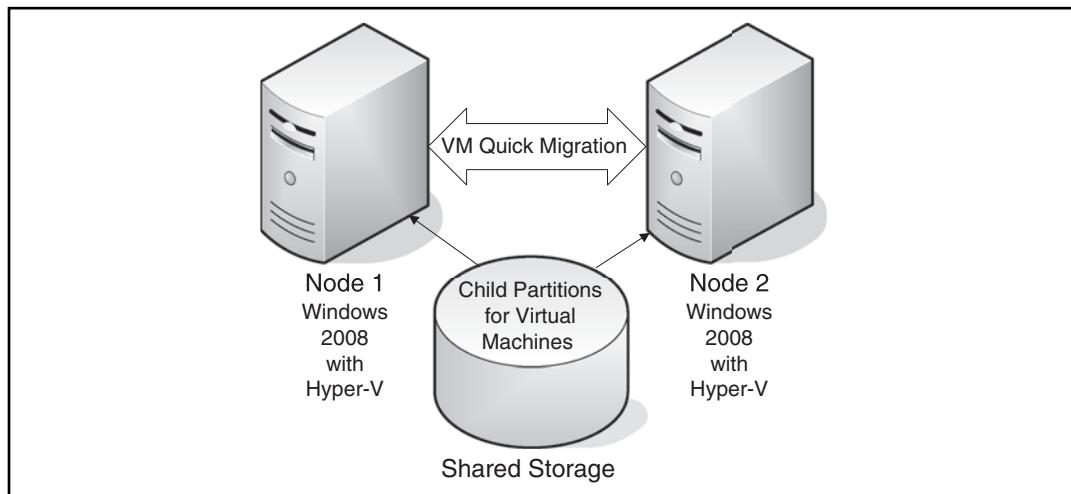
Virtualization and High Availability

The addition of the Hyper-V Virtualization solution in Windows 2008 Server has allowed for a new way to use Failover Clustering to accomplish High Availability solutions (see Figure 9.22). Windows 2008 Servers configured for the Hyper-V Role can now be configured as nodes in a failover cluster. This configuration allows for the Child Partitions containing the Virtual Machines to be hosted on a share storage platform that is equally available to each host. At any one time, only one of the cluster nodes will actually host the running VMs in an Active Passive mode configuration. This allows for the use of Hyper-V's Quick Migration functionality, where running VMs can be migrated from one host Node to the other without the requirement to be shut down.

NOTE

A short period of interruption in the availability of the Virtual Machine being migrated will be experienced during this process. This period of service interruption will vary between a few seconds to as much as 30 seconds, depending on the class of hardware, and available resources of the host machines.

Figure 9.22 High Availability with Hyper-V Architecture



The most significant advantage of this arrangement, beyond the obvious increase in the expected level of availability for the Virtual Machines running on this platform, is the fact that administrative actions and maintenance can now be performed on the host nodes, with minimal interruption to the Virtual Machines running on them. When administrative tasks such as O/S patching are necessary, the guest VMs can be migrated over to the alternate host node, in order to facilitate maintenance.

Planning for Backup and Recovery

Windows 2008 Server backup functionality has been redesigned to use the new Windows Server Backup Utility, as opposed to the NTBackup utility offered with previous versions of Windows. Windows Server Backup has been designed with the

intent not only to simplify the process of backing up and restoring data, but also to provide enhanced reliability for the results of these operations. Windows Server Backup is an optional feature in Windows 2008 Server.

Windows Server Backup uses Volume Shadow Copy Services (VSS) to accomplish its function, and backs up to the VHD File format. It can be used either for individual object, full volume, or full server recovery, called a “Bare Metal Restore.” These options will be discussed later in this section. It can be installed via one of the following three methods:

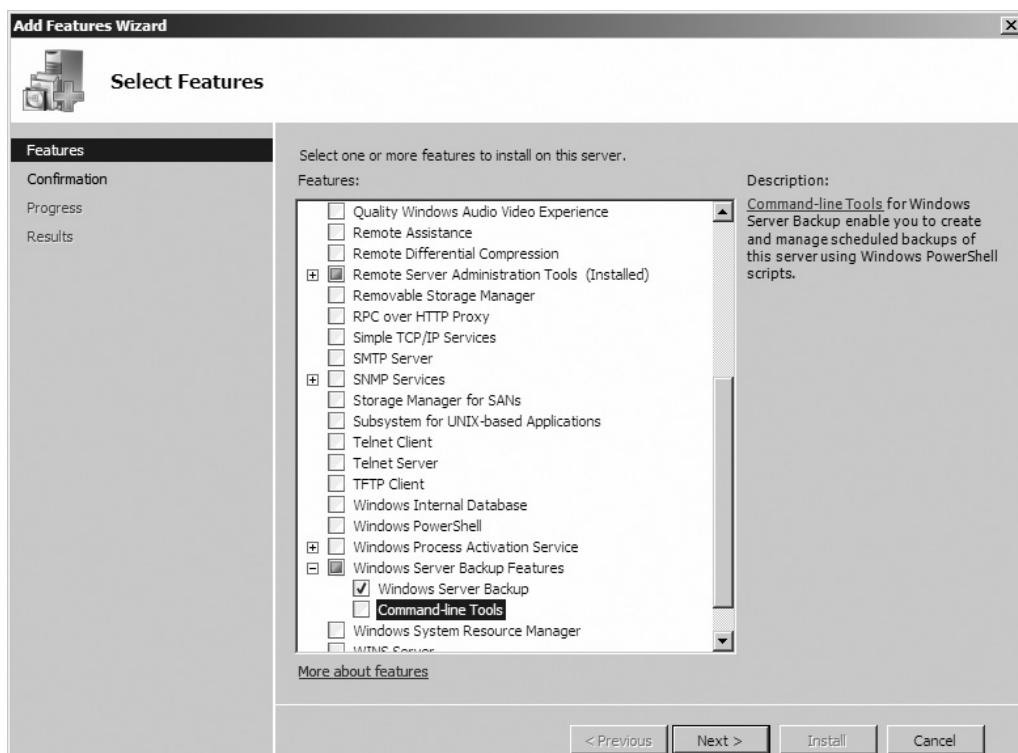
- **Initial Configuration Tasks Window** The Initial Configuration Tasks Screen that appears on the desktop after login provides the option to install Windows Server Backup by selecting **Add Features | Windows Server Backup Features | Windows Server Backup**.
- **Server Manager** Server Manager provides the option to install Windows Server Backup by selecting **Start | Administrative Tools | Features | Add Features | Windows Server Backup Features | Windows Server Backup**.
- **Command Line** Windows Server Backup can also be installed from the command line using the ServerManagerCmd.exe tool.

EXERCISE 9.3

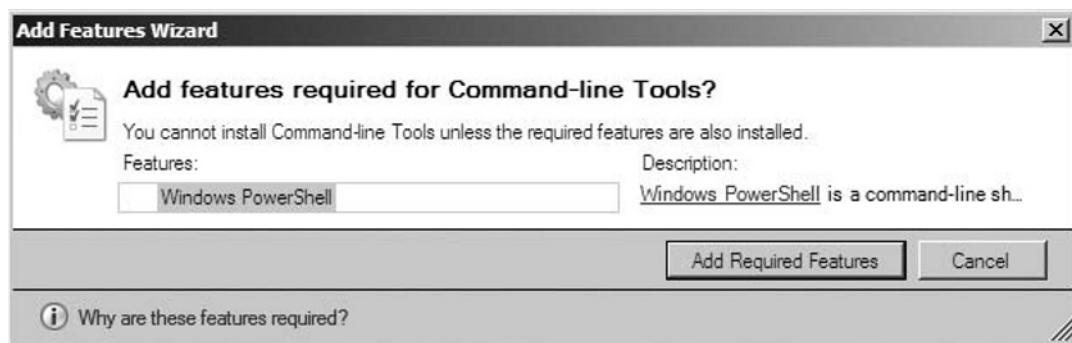
INSTALLING THE WINDOWS SERVER BACKUP FEATURE ON A FULL INSTALLATION OF WINDOWS 2008 SERVER

As a prerequisite this exercise assumes the pre-existence of a full installation of Windows 2008 Server that has been fully configured with all supporting requirements in place.

1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Features | Add Features**.
3. In the **Add Features** page that appears, select **Windows Server Backup Features | Windows Server Backup**. Also select **Command Line Tools** under the same heading (see Figure 9.23).

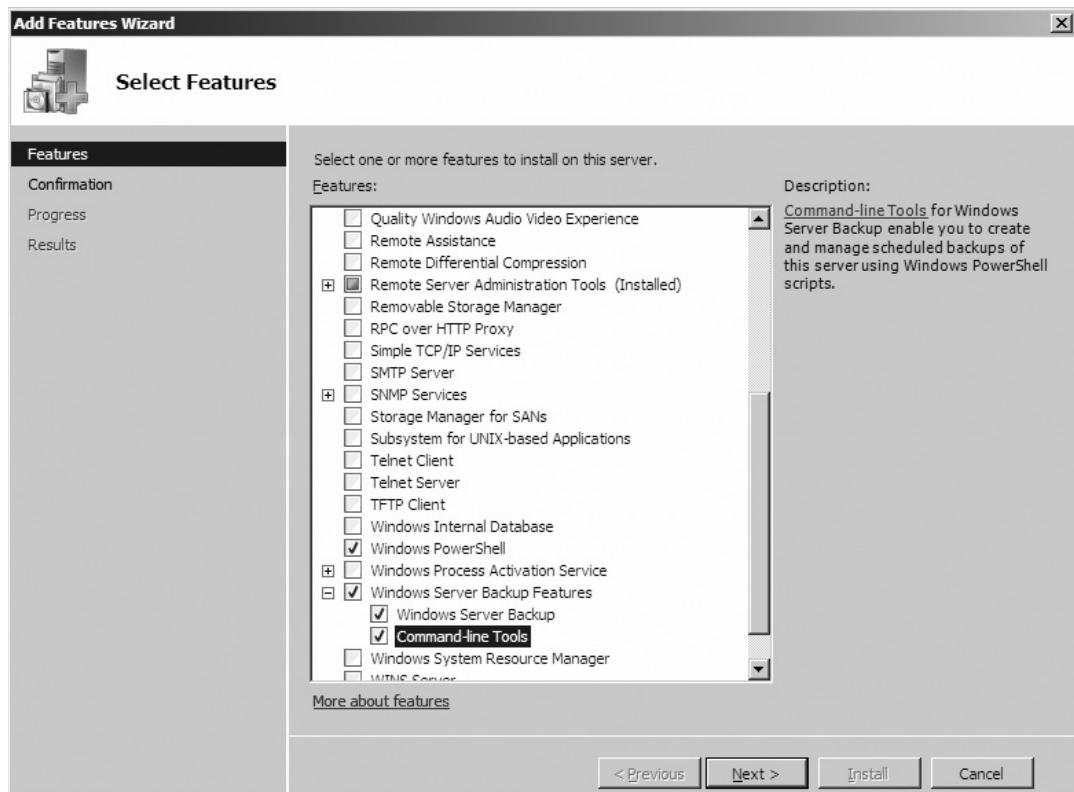
Figure 9.23 Server Manager “Select Features” Wizard

4. As soon as **Command Line Tools** is selected, a secondary window will appear indicating a dependency upon the **Windows PowerShell** feature. Click **Yes** to add this dependant feature (see Figure 9.24).

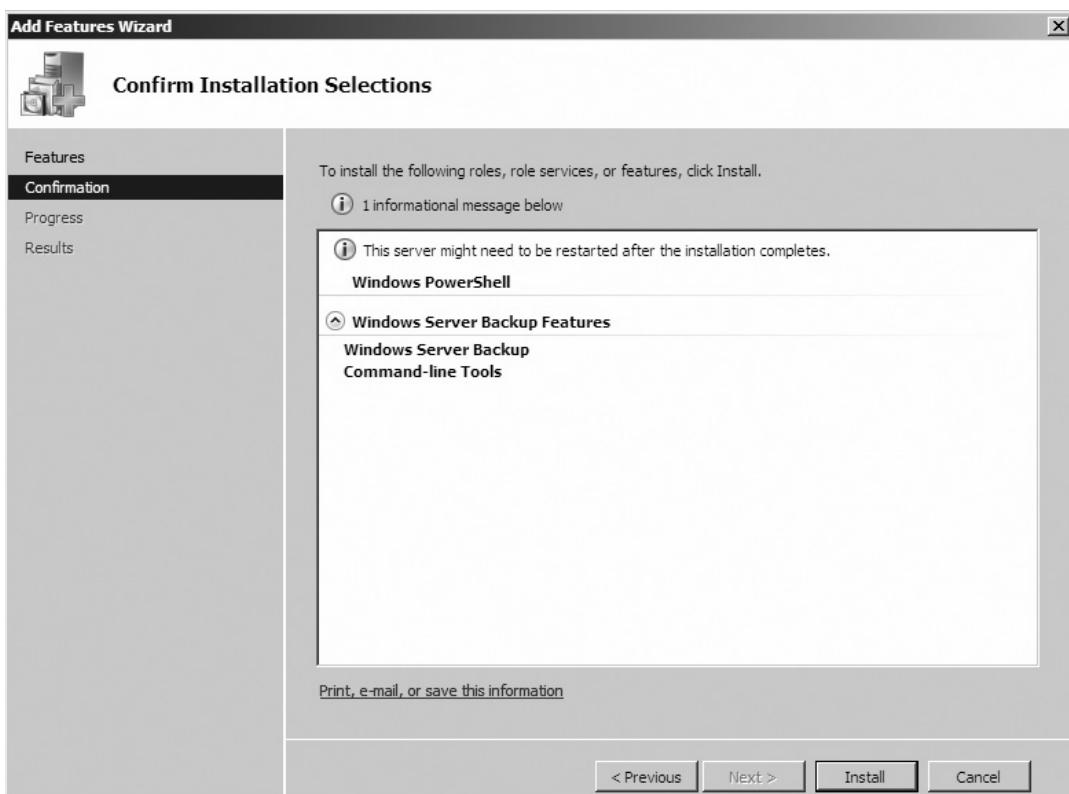
Figure 9.24 Add Features Wizard “Add Features Required For Command-Line Tools?”

5. Once the additional **Command Line Tools** option has been successfully added, select **Next** to continue (see Figure 9.25).

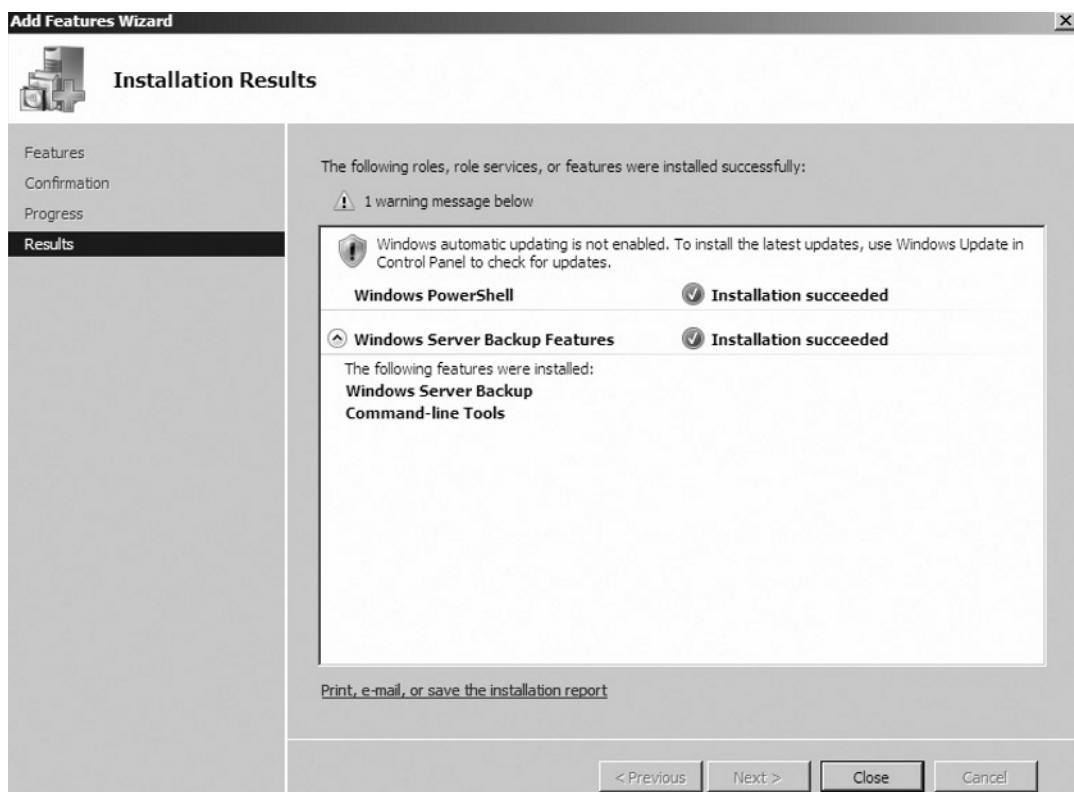
Figure 9.25 Add Features Wizard “Select Features” Page



6. In the **Confirm Installation Selections** page verify that the correct options have been chosen, and then select **Install** to proceed, as seen in Figure 9.26.

Figure 9.26 Add Features Wizard “Confirm Installation Selections” Page

7. Once the installation has completed, select **Close** to complete the installation process (see Figure 9.27).

Figure 9.27 Add Features Wizard “Installation Results” Page

-
8. The Windows Server Backup Feature has now been successfully installed on your server.

EXERCISE 9.4

PERFORMING A FULL SERVER BACKUP USING THE WINDOWS SERVER BACKUP GUI UTILITY ON A FULL INSTALLATION OF WINDOWS 2008 SERVER

As a prerequisite this exercise assumes the pre-existence of a full installation of Windows 2008 Server, as well as successful completion of the previous procedure to install the Windows Server Backup feature.

NOTE

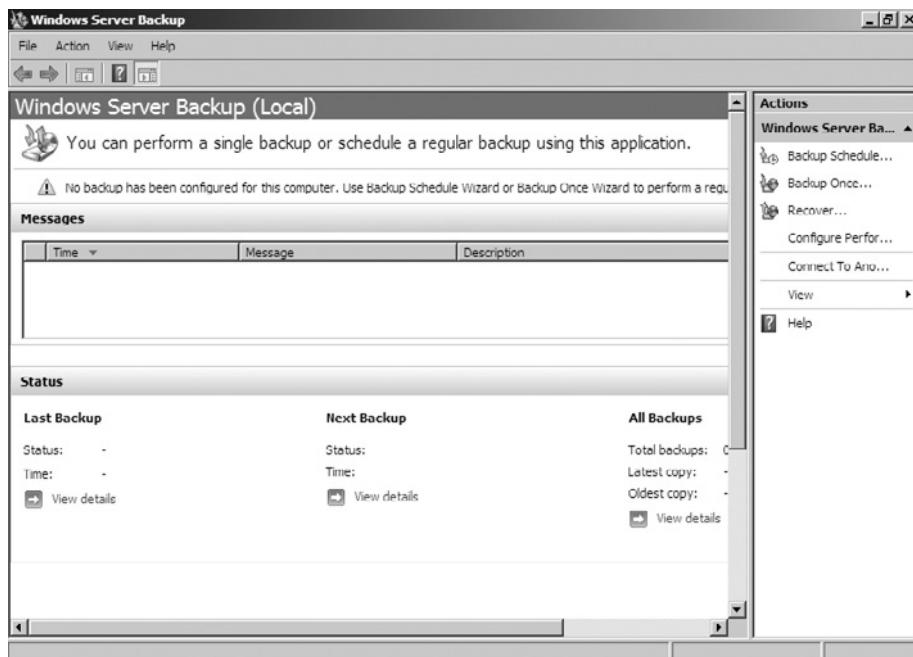
Windows Server Backup Utility provided with Windows 2008 Server does not support “Backup to Tape” functionality

TEST DAY TIP

The Windows Server Backup Utility takes only one full snapshot of a volume. After that it's just differentials.

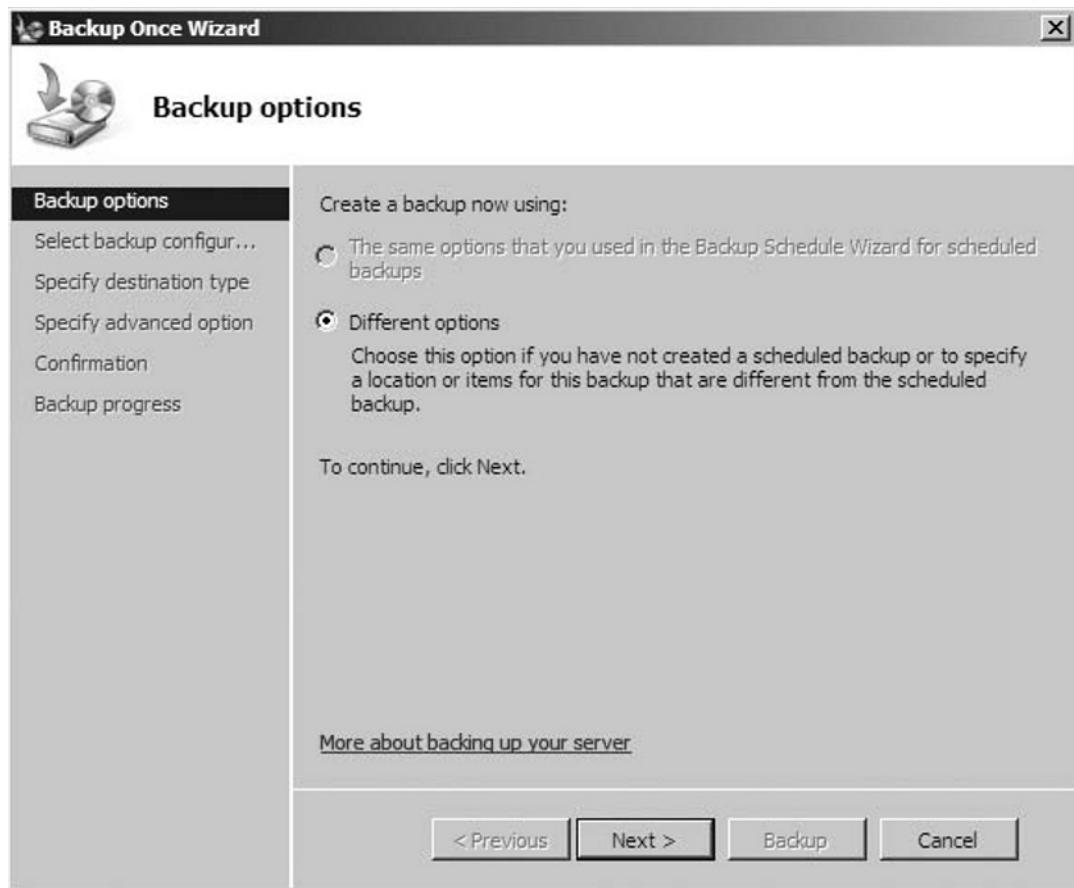
1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Windows Server Backup**.
3. In the **Actions** Pane to the upper right, select **Backup Once** (see Figure 9.28).

Figure 9.28 Windows Server Backup Manager Page



4. Since this is the first backup to be carried out, the **Different Options** will be the default method available for backing up the server.
5. Select **Next** to proceed (see Figure 9.29).

Figure 9.29 Backup Once Wizard “Backup Options”

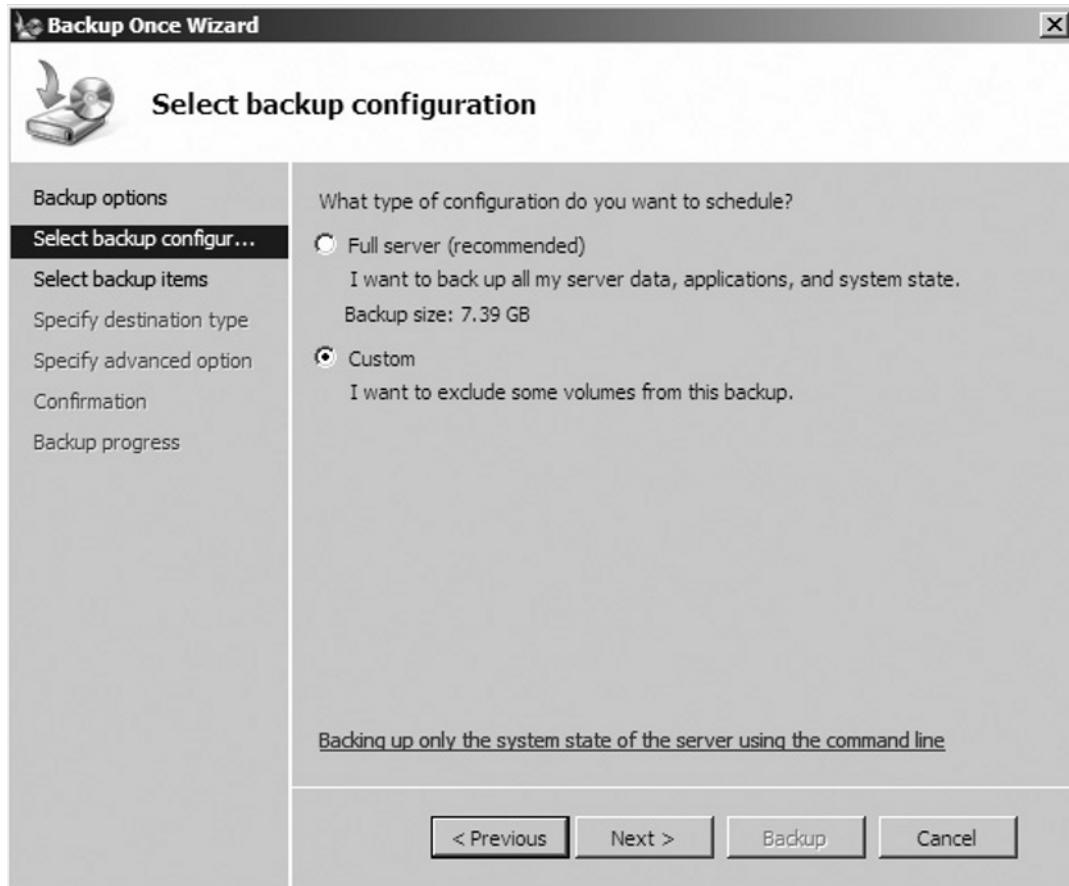


NOTE

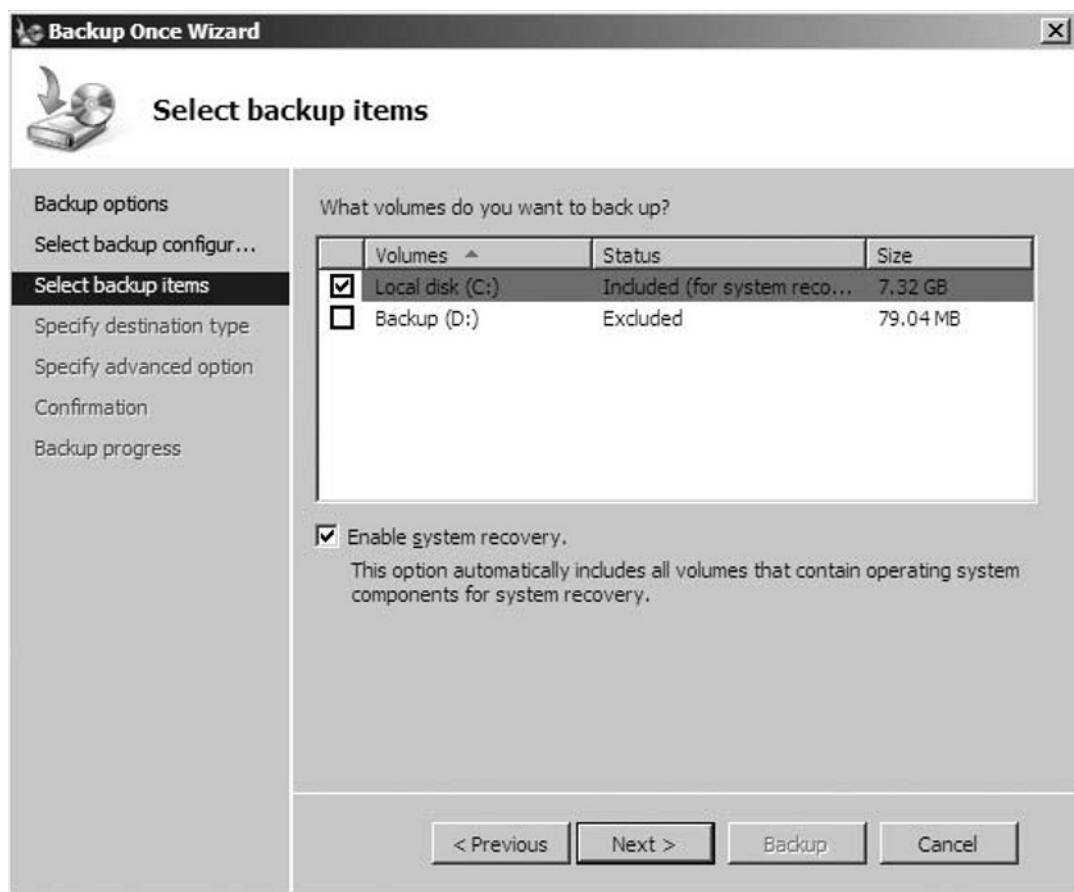
For subsequent backups the **same options** selection will be available, since there will then be selections available from previous backups that can be repeated if desired. On the first backup, **Different Options** is the only available selection since there are no historical settings available for selection at this point.

6. In the **Select Backup Configuration** Page select **Full Server**.
7. Select **Next** to proceed (see Figure 9.30).

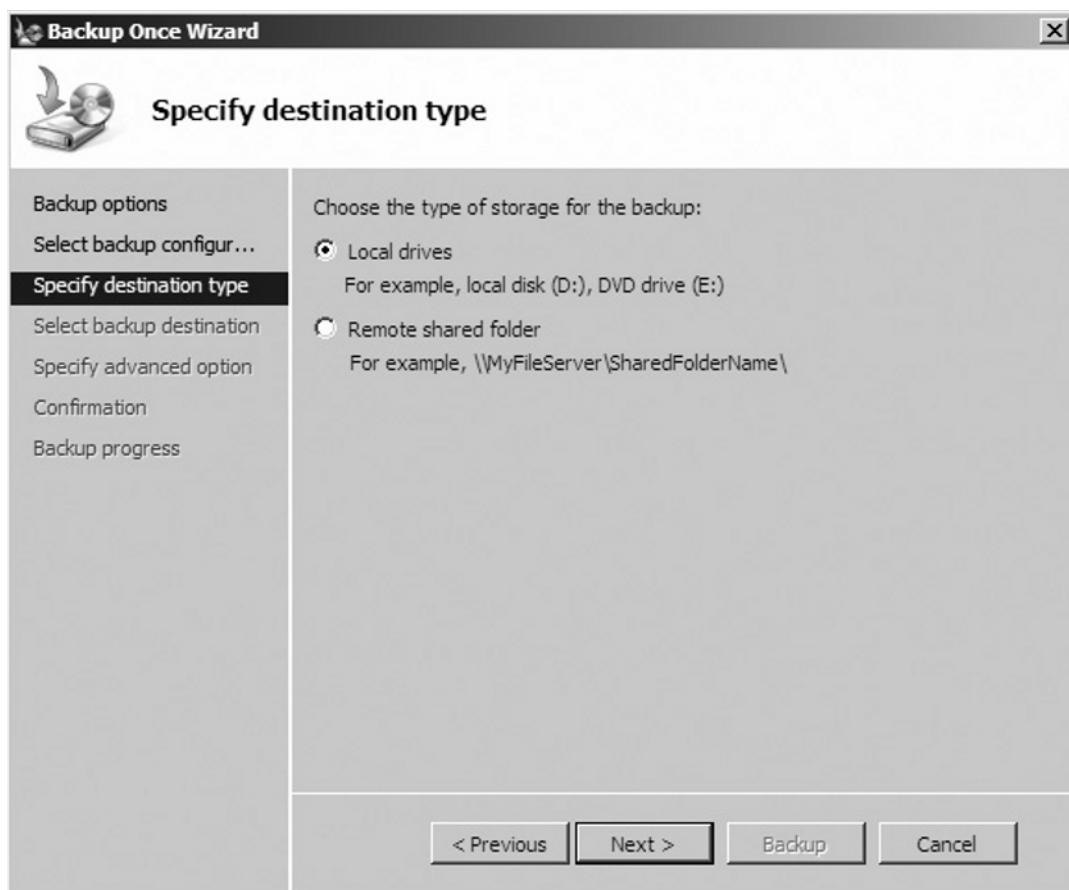
Figure 9.30 Backup Once Wizard “Select Backup Configuration” Page



8. When asked what volumes you wish to backup, select the system drive, and ensure that **Enable System Recovery** is checked.
9. Select **Next** to proceed (see Figure 9.31).

Figure 9.31 Backup Once Wizard “Select Backup Items” Page

10. In the **Specify Destination Type** page select **Local Drives** as the type of storage for backup.
11. Select **Next** to proceed (see Figure 9.32).

Figure 9.32 Backup Once Wizard “Specify Destination Type” Page

12. In the **Specify Backup Destination** page select **Local Drives** to which you want the backup file to be copied.
13. Select **Next** to proceed (see Figure 9.33).

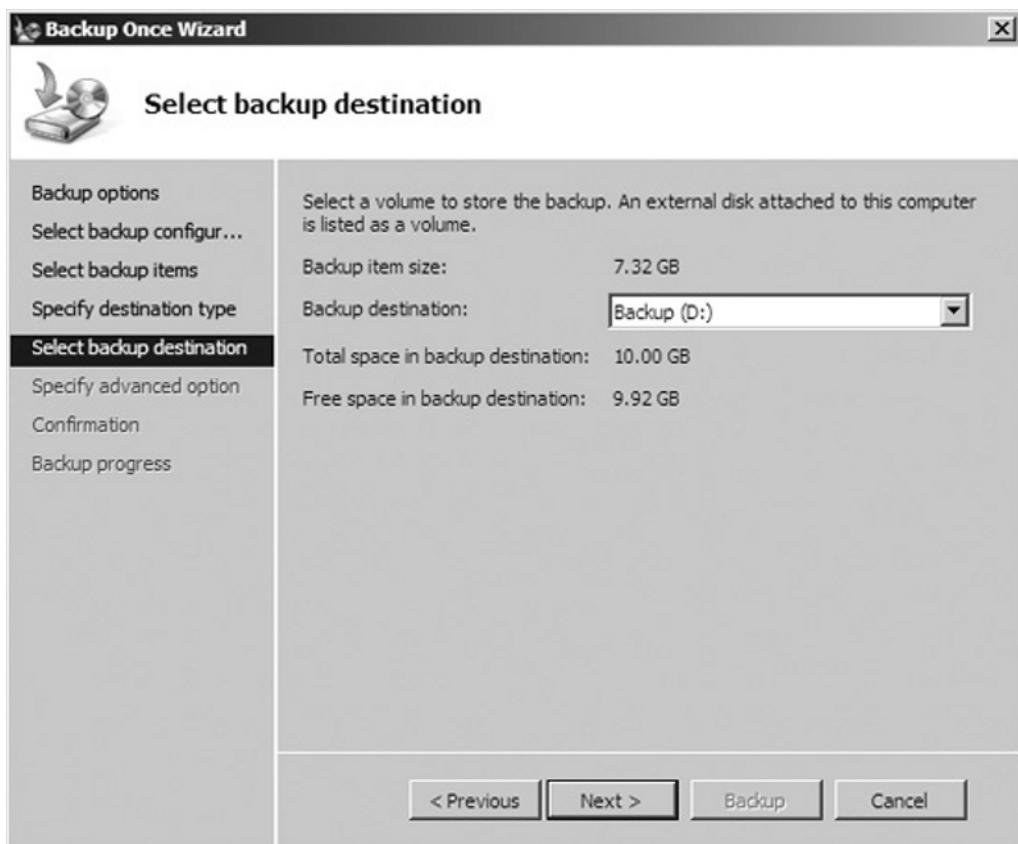
TEST DAY TIP

The selected local drive must not be the same drive from which files are being backed up. Any attempt to back files up, and copy them to the same drive from which they are being backed up, will be met with an error message.

NOTE

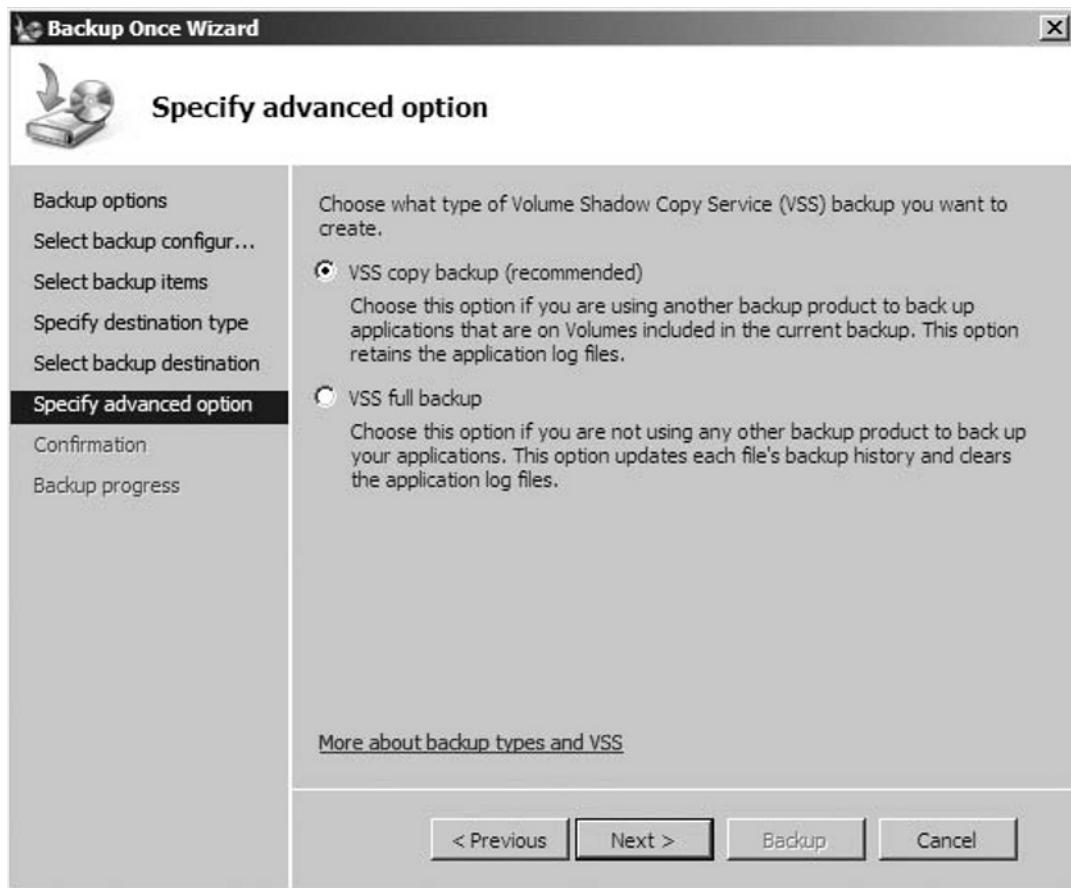
It is possible to override this limitation, by making a change in the registry. Microsoft's KB Article 944530 describes how to accomplish this change.

Figure 9.33 Backup Once Wizard "Specify Backup Destination" Page

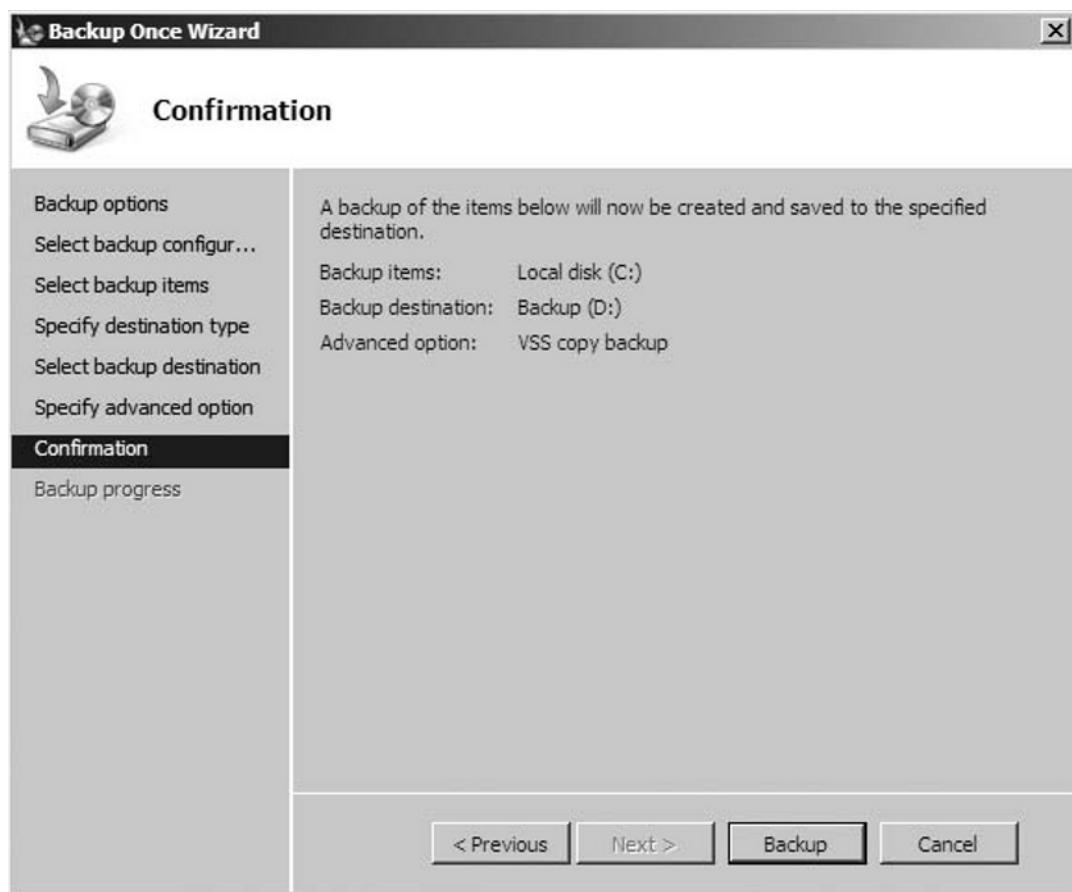


14. In the **Specify Advanced Option** page select **VSS Copy Backup**.
15. Select **Next** to proceed (see Figure 9.34).

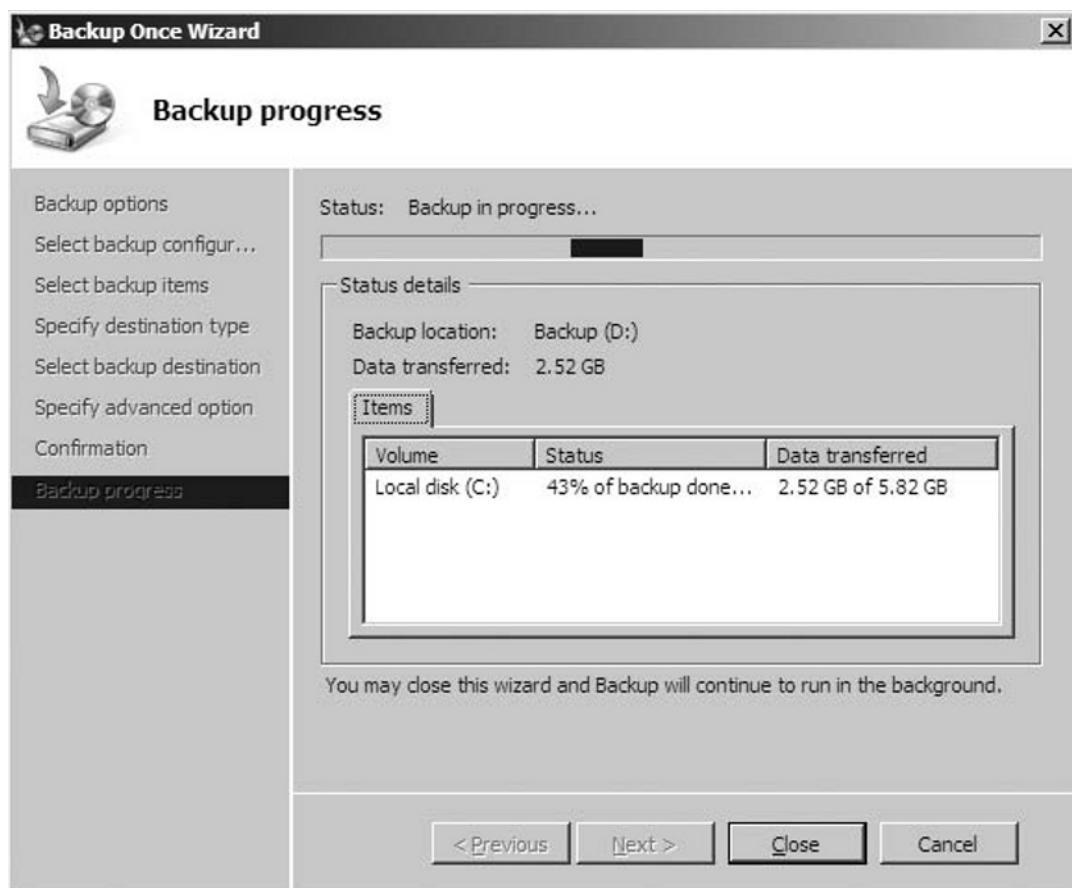
Figure 9.34 Backup Once Wizard “Specify Advanced Option” Page



16. On the **Confirmation Page** review all selected options
17. Select **Next** to proceed (see Figure 9.35).

Figure 9.35 Backup Once Wizard “Confirmation” Page

18. The **Backup Progress** page will then be displayed showing the details and progress.
19. Once the backup reports as complete, select **Close** to complete the process (see Figure 9.36).

Figure 9.36 Backup Once Wizard “Backup Progress” Page

-
20. The Full Server Backup of your Windows 2008 Server using Windows Server Backup has now been successfully completed.

Data Recovery Strategies

The demands and expectations placed upon the backup solutions of modern organizations have evolved rapidly in recent years. The requirements for backup and restoring performance have greatly increased in response to the significant rise in the quantities of data needing to be backed up. As organizations grow, and data storage technology develops ever-increasing capacity, not only is there more to be backed up, but the speeds at which it can be backed up, or recovered in the event of a failure, have also become of critical importance. Disk to Disk to Tape solutions are being employed in many larger organizations in order to overcome the limited performance of the traditional Disk to Tape solutions. New and interesting advancements introduced with Windows Server 2008 have served even more so to increase the performance demands being placed on backup and restore systems.

While specific backup and restore technologies may improve steadily, the traditional method of scheduled full and incremental backups with selected versions kept offsite for disaster recovery purposes will remain the industry standard most certainly for the foreseeable future. There are however some new and unique challenges being brought about by the advent of new technologies, and solutions that must be considered separately.

First is the introduction of the Windows 2008 Server Core installation. Unlike previous versions the Server Core installation is a bare-bones version of the new Windows operating system, with nothing but the minimum required services running on it. While the Windows Server Backup utility can be installed, the methods of access and use will change, as will the requirement for administrative user knowledge regarding methods and implementation. This is a factor that will undoubtedly affect other traditional strategies involving third party backup utilities as well.

The most significant change being presented with respect to the effect on backup strategies is the advent of virtualization technology. Virtualization is causing a shift in the thinking and practices that need to be applied to the protection of individual server workloads from unexpected events like hardware loss, accidental deletions, and so on. It is now necessary to think not just about the important files contained within a server, but about the safeguarding and backup of the server itself. Given the fact that the primary content of a virtual server is contained within one single file, consideration now needs to be given to how to backup that individual file, with the intent to be able to recover it quickly to any alternate hardware platform in the event of a hardware loss, unexpected disaster, etc.

The following options exist for the backup of virtualized server workloads:

- **Traditional Agent based backups** The standard method of installing a third party backup agent or using Windows Server Backup to backup the internal contents of a server and store those contents in an alternate location is still a common approach, but it does have its limitations. The use of this option does not provide the ability to take advantage of the virtualized file format. What this means is that if an entire server is lost, then time is also lost recreating a replacement server, and then restoring the backups to it.
- **Snapshots and/or Cloning** The ability to take snapshots of virtual machines, as well as to create exact copies of them using cloning technology, means that a full server recovery to the state it was at when the last snapshot or clone was created can be accomplished very quickly, and easily.
- **A Combination of Snapshots and/or Cloning and Traditional Agent-based Backups** The cloning or snapshooting of virtual machines can allow for a full server recovery to be accomplished very quickly, and easily. At the same time cloning or snapshooting on a daily basis would undoubtedly present some challenges with respect to the amount of storage space and administrative effort that would be required to maintain the solution. This is where the traditional method of backing up the internal contents of a server using either a third party utility or Windows Server Backup can provide the additional functionality needed to bring a recovered server completely up-to-date in the wake of any sort of loss.

Server Recovery

The functionality provided in the Windows Server Backup Utility for the recovery of an entire server in the wake of hardware failure or similar event is called the **Bare Metal Restore** procedure. There are many options involving the use of third party utilities for the full recovery of a server that has been lost due to some unexpected event, however many smaller companies rely on the Windows Server Backup function to protect them from the results of such events.

A “Bare Metal Restore” can be accomplished using any of the following methods:

- **WinRE (Windows Recovery Environment)** The WinRE recovery environment provides the option to start a server and perform a full “Bare Metal Restore” when the server is either completely lost, or in a non-startable state.
- **Command Line** A full Bare Metal Restore of a server can be accomplished at the command line using the wbadmin.exe utility.

WinRE Recovery Environment Bare Metal Restore

The WinRE recovery environment is designed to allow for the full recovery of all operating system level files to a server by providing a separate boot environment in which the computer can be started without actually starting any of the operating system files which are targeted for recovery. By preventing the startup and execution of any actual operating system files this allows for the O/S files to be processed for restore while they are in a completely non-running state, not locked by any processes. While the Bare Metal Restore procedure is designed to recover all files on a computer including any data, it is the O/S files that most commonly must be maintained in a non-running state in order to get a clean result from the restore procedure.

To perform a full server Bare Metal Restore recovery of a server using **WinRE Recovery Environment**, perform the following actions:

1. Boot the server to the Windows 2008 Server Media.
2. At the opening **Windows installation** screen, accept all options and click **Next**.
3. At the **Install Now** page, select **Repair your Computer**.
4. On the **System Recovery Options** page click outside the box to clear all selections, and then click **Next**.
5. When asked to **Choose a Recovery Tool**, select **Windows Complete PC Restore**.
6. Select **Restore a Different Backup** and then click **Next**.
7. On the **Select the Location of the Backup** page browse to the backup file location (assumes that the backup file is stored locally) then select **Next**.
8. Select the specific Backup File to restore, and then choose **Next**.
9. On the **Choose How to Restore the Backup** page select one of the following options:
 - A. **Format and Repartition Disks** to replace all data on all volumes.
 - B. **Exclude Disks** then select the specific disks that you want to exclude.
10. Select **Next**, and then **Finish**.
11. When prompted select **I Confirm That I Want to Format the Disks and Restore the Backup** and then **OK** to proceed.

Command Line Bare Metal Restore

To perform a full server, “Bare Metal Restore” recovery of a server using the Command Line utility, use the following commands:

```
wbadmin getversions -backuptarget<drive letter>  
wbadminstart BMR -version<versioned> -backuptarget<drive letter>  
restoreallvolumes -recreatedisks
```

Recovering Directory Services

Directory Services backup and recovery is accomplished somewhat differently in Windows 2008 Server than it has been in previous versions of Windows Server.

First is the use of the new Windows Server Backup functionality, which although it accomplishes essentially the same tasks, is designed to do so in a somewhat different and simplified manner over previous versions. Windows 2008 Server has been designed to concentrate on the backup of “Critical Volumes” for the security of important files, and functionality. The Active directory-specific Critical Volumes and their files that are targeted by the backup utility include the following:

- SYSVOL Volume
- BOOT Volume
- SYSVOL Tree
- NTDS.dit Database
- NTDS Log Files

The principles of Directory Services backup and recovery remain much the same, but Windows Server Backup introduces a slightly altered procedure to accomplish DS Backup and recovery requirements.

Backup Methods for Directory Services

There are two different methods available to accomplish the backup of Directory Services:

- **Windows Server Backup GUI Utility** Windows Server Backup GUI allows for both one-time and scheduled backups of the files necessary to backup important Directory Services files.
- **Command Line Backup Utility** The Command Line backup utility is called wbadmin.exe. It provides all of the same functionality as the GUI utility.

Backup Types for Directory Services

Directory Services can be backed up in either of two different ways in Windows 2008 Server.

- **Critical Volume Backup** A Critical Volume backup of a Domain Controller provides the option to recovery Directory Services using the Directory Services Restore Mode method Directory services in the event of a hardware failure or accidental deletion of a Directory Services object
- **Full Backup** A full backup of all server volumes provides the ability to perform either a Bare Metal Restore recovery or a Directory Service Restore Mode recovery of Directory services in the event of a hardware failure or accidental deletion of a Directory Services object.

Recovery Methods for Directory Services

There are two primary options available for the recovery of Directory Services in Windows 2008 Server:

- **Directory Services Restore Mode** Directory Services Restore Mode can be accessed by selecting F8 when prompted during bootup on a Domain Controller
- **Full Server Recovery** A “Bare Metal Restore” is the procedure that would be applied in the event that the subject server is not in a state where it can be started to get it into Directory Services Restore Mode.

NOTE

See the previously discussed “Server Recovery” segment for details regarding how to accomplish the prerequisite steps for this type of Directory Services Restore.

Directory Services Restore Mode Recovery

There are two main types of Directory Services restore that are available options for recovery of Directory Services in the wake of any unforeseen event, accidental directory object deletions, etc. They are as follows:

- **Non-Authoritative Restore** A Non-Authoritative restore of Directory services is the desired method to be employed when other domain controllers are available in the domain to replicate up-to-date changes to the directory after the restore has been completed. This method is the option to be chosen when one DC in a set has been lost due to hardware failure, or some other similar event. It is designed to bring Directory Services back up to a running state on one specific DC, with the intent to allow the others to bring it back in sync after the restore via replication. This would not be the method to be used in a scenario where there is only one domain controller, and it is the one being restored.
- **Authoritative Restore** An authoritative restore of Directory Services is the desired method of Directory Services recovery in either of the following two scenarios:
 - **Accidental Deletion of a DS Object** An authoritative Restore is the desired method to be employed when a Directory Services restore is necessary in order to accomplish the recovery of just one or a specific group of Active Directory objects. In this scenario, the authoritative procedure allows for these specific objects to be marked as authoritative, thus preventing them from being overwritten by replication changes forwarded by other DCs in the domain, such as happens when a non-authoritative restore procedure is carried out.
 - **Recovery of the sole DC in a Domain** An authoritative Restore is the desired method to be employed when a domain contains only one domain controller that has been lost for any reason. While not identical to the authoritative procedure used to recover a deleted object, it is still necessary to take additional steps beyond a basic non-authoritative restore in this particular circumstance. This is because the non-authoritative restore procedure for Directory Services leaves directory services in a state that is looking for updates from other domain controllers. If a DC being restored is the only one in the domain, it is necessary to take steps to let it know not to look for updates after the restore. This is done by setting a parameter called the *burflags value*.

Non-Authoritative Restore

A Non-Authoritative restore of Directory Services Restore Mode can be accomplished by either of two methods. Here are the steps for the first method:

1. Reboot the Domain controller, and select **F8** on startup for the **Boot Options** Menu.
2. Select Directory Services Restore Mode.
3. When prompted type in the **Directory Services Restore Mode Password**. (This password would have been created during the initial DC Promotion Process.)
4. Select the appropriate backup file, and restore it using the **Windows Server Backup | Restore Wizard**.
5. When completed, reboot the server, and allow Active Directory time to replicate changes.

Here are the steps for the second method:

1. From the Start Menu select **Switch User** and then **Other User**.
2. Enter **.\administrator**, and then provide the **DSRM password** when prompted.
3. Open the **Command Prompt**, select **Run as Administrator**, and type the following:

```
wbadm getversions -backuptarget<targetdrive>
-machin:<backupcomputername>
```
4. When prompted for sources type the following command:

```
wbadm start systemstaterecovery -version:<MM:DD:YYYY-HH-MM>
-backuptarget:<targetdrive> -machin:<backupcomputername>
-quiet
```
5. After the recovery has completed, restart the server.
6. When the login prompt appears, select **Switch User** once again to allow type in the **Directory Services Restore Mode Password**. (This password would have been created during the initial DC Promotion Process.)
7. Select the appropriate backup file, and restore it using the **Windows Server Backup | Restore Wizard**.
8. When completed, reboot the server, and allow Active Directory time to replicate changes.

Authoritative Restore

The following is the procedure for accomplishing an authoritative restore of Active Directory Services:

1. First it is necessary to perform the Non-Authoritative restore procedure, by using either of the previously mentioned methods
2. After the restoration has been completed, but prior to restarting the server use the **ntdsutil authoritative restore** command to identify and mark the specific Directory Services objects that need to be recovered.
3. Once completed, restart the Domain Controller.
4. Once up and running, login and verify that the specific objects that were marked for Authoritative Restoration are once again present in AD.

Object Level Recovery

As was seen in the previous segment, Windows Server Backup is an optional feature in Windows 2008 Server that must be installed prior to its use. Once this feature has been successfully installed, then regular or one-time backups of individual files will be an available function. While many third-party high-end solutions are available for the backup of the content of entire servers, there will always be a requirement for a utility such as Windows Server Backup to provide support for the backup and restore requirements of administrators performing “one time maintenance” to servers or specific files. As well, for smaller organizations that cannot afford the high cost solutions provided by many of these third-party vendors, Windows Server Backup can provide an acceptable option for them to protect their assets from unforeseen failures or events.

EXERCISE 9.5

PERFORMING THE OBJECT LEVEL RECOVERY OF INDIVIDUAL FILES USING THE WINDOWS SERVER BACKUP UTILITY ON A FULL INSTALLATION OF WINDOWS 2008 SERVER

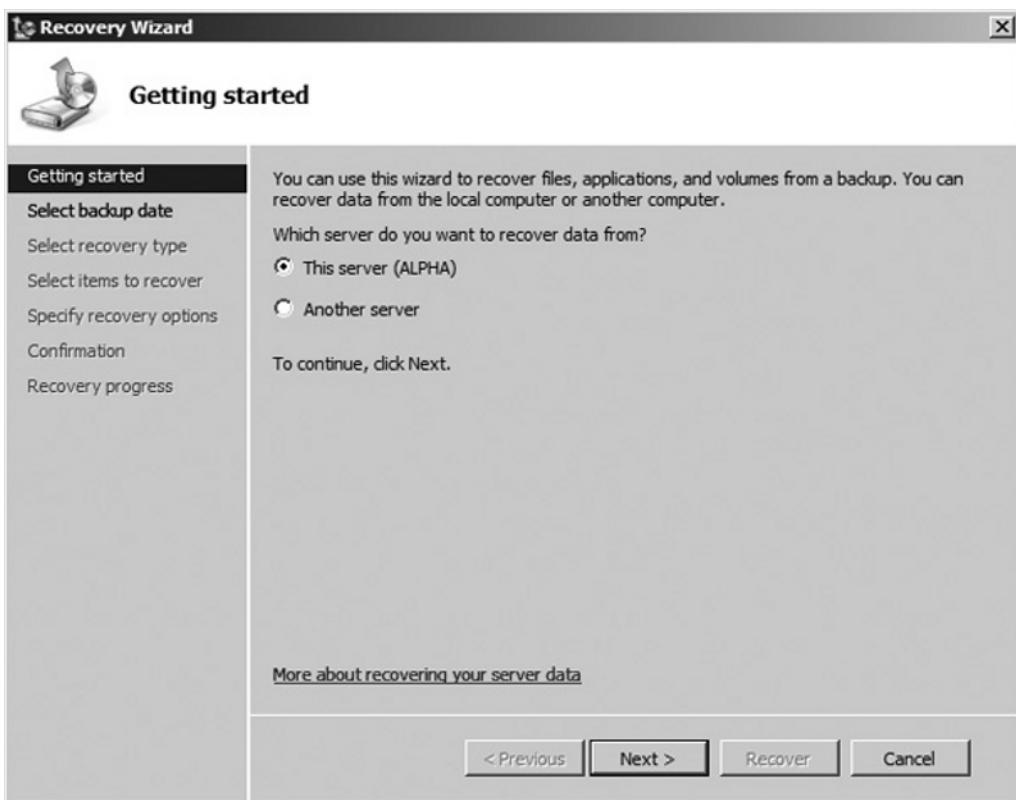
As a prerequisite this exercise assumes the pre-existence of a full installation of Windows 2008 Server, as well as completion of the previous procedure to install the Windows Server Backup feature, and availability of a valid backup of the subject files.

TEST DAY TIP

The Windows Server Backup Utility takes only one full snapshot of a volume. After that it's just differentials. For this reason, it is necessary to take note of when the last Full Backup was performed on the subject files. If the desired version was backed up multiple times since the last Full Backup, then it will be necessary to restore the Full Backup, as well as the appropriate Incremental Backups that followed the last Full Backup.

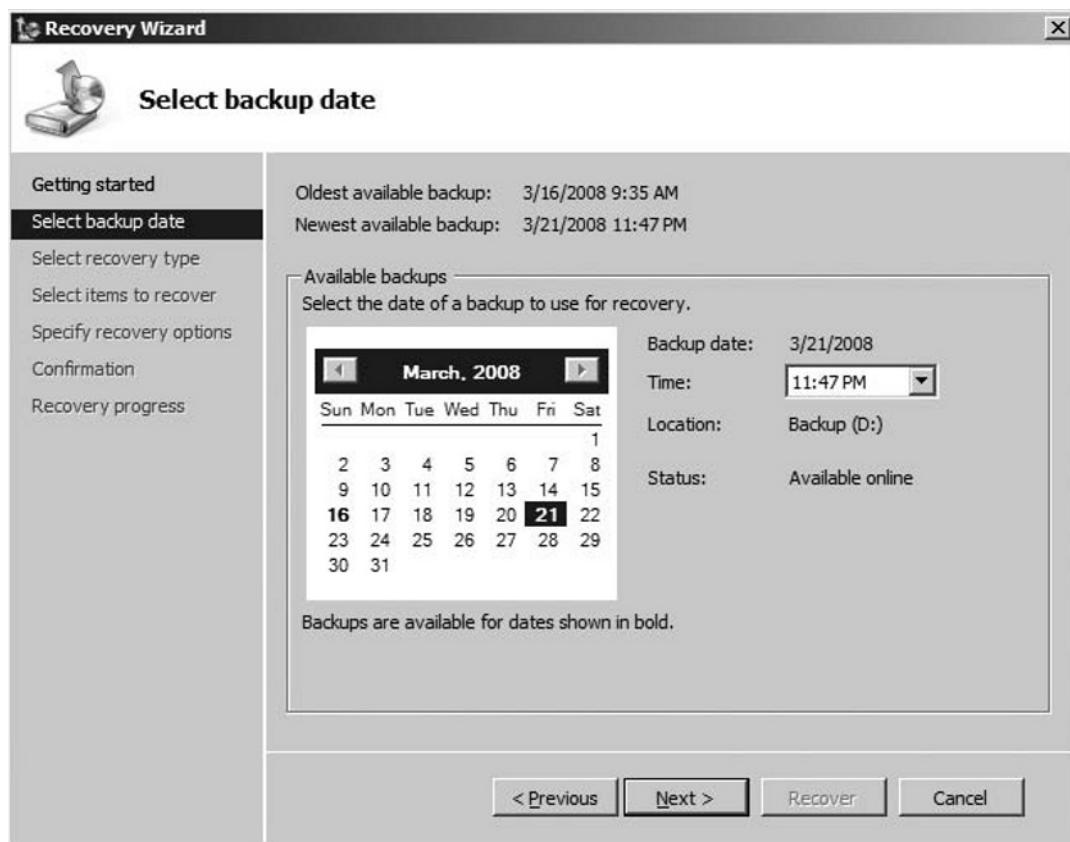
1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Windows Server Backup**.
3. In the Actions pane to the upper right, select **Recovery Wizard** (see Figure 9.37).

Figure 9.37 Windows Server Backup—Recovery Wizard
“Getting Started” Page



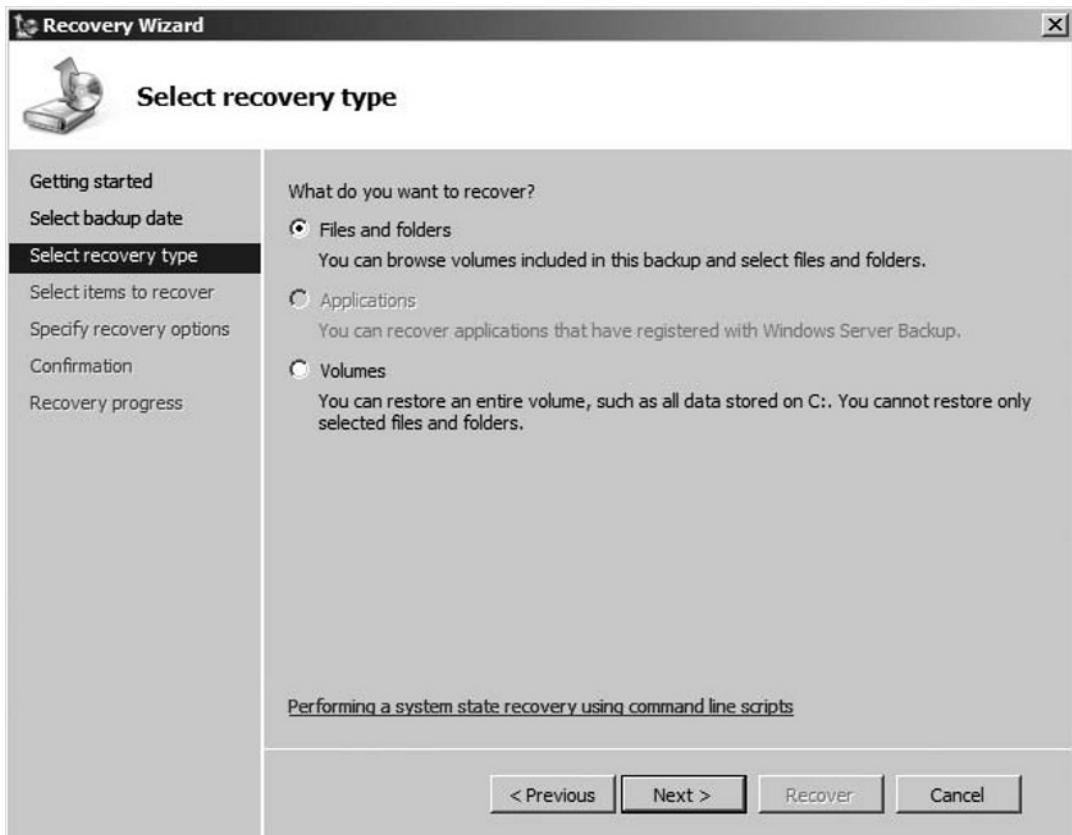
4. In the Select Backup Date page, choose the date for your backup (see Figure 9.38).

Figure 9.38 Windows Server Backup—Recovery Wizard “Select Backup Date” Page



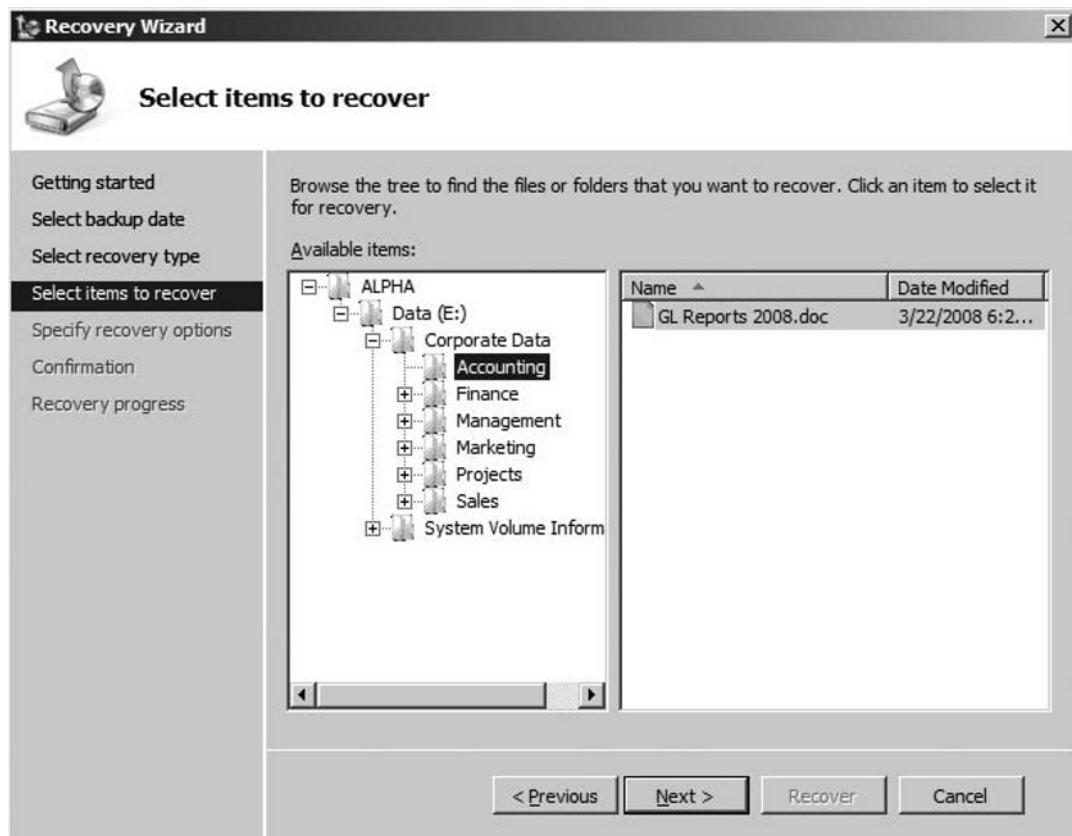
5. Select your recovery type (see Figure 9.39).

Figure 9.39 Windows Server Backup—Recovery Wizard
“Select Recovery Type” Page



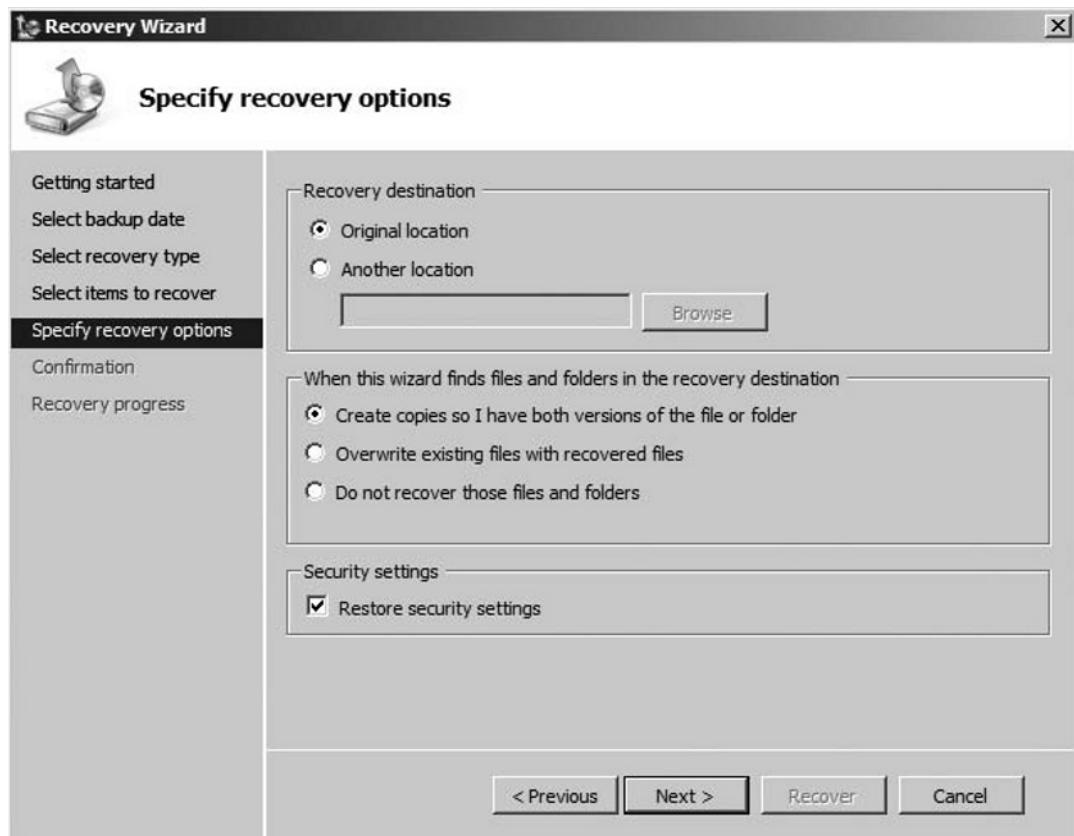
6. Select your items to recover (see Figure 9.40).

Figure 9.40 Windows Server Backup—Recovery Wizard
“Select Items to Recover” Page



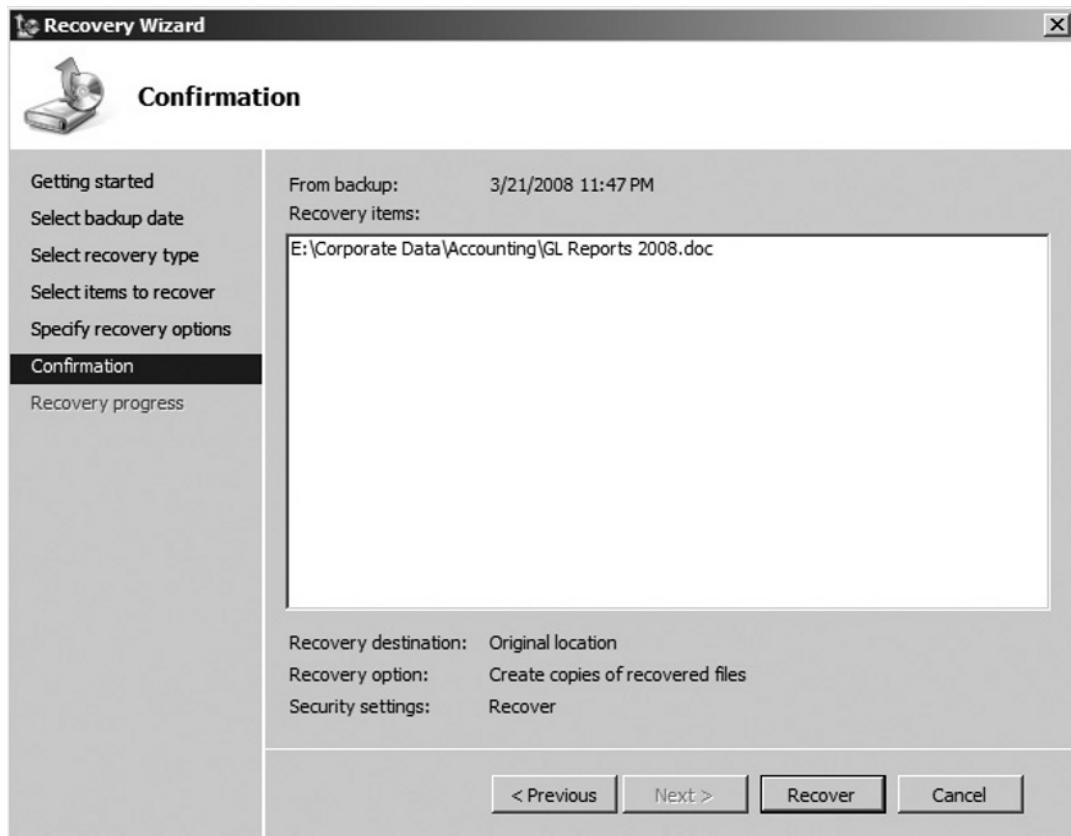
7. Specify your recovery options and click **Next** (see Figure 9.41).

Figure 9.41 Windows Server Backup—Recovery Wizard “Specify Recovery Options” Page



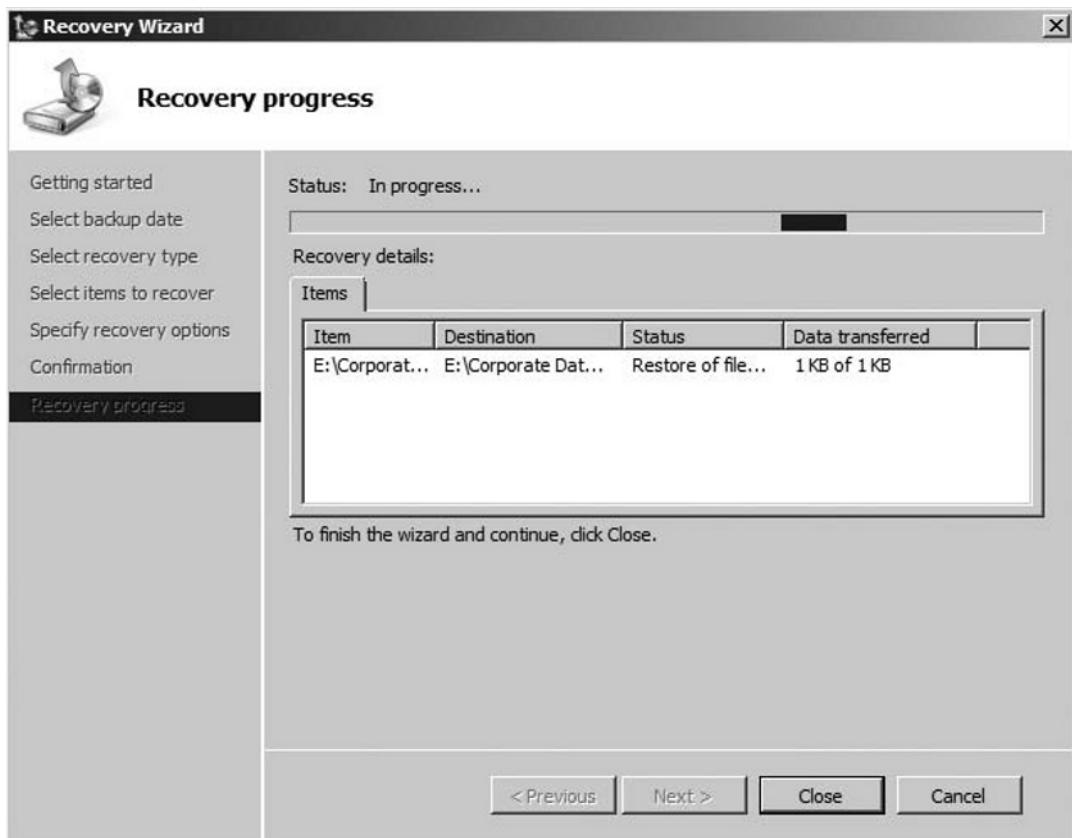
8. View the **Confirmation** page and then choose **Recover** (see Figure 9.42).

Figure 9.42 Windows Server Backup—Recovery Wizard “Confirmation” Page



9. View the status on the **Recovery Progress** page (see Figure 9.43).

Figure 9.43 Windows Server Backup—Recovery Wizard “Recovery Progress” Page



10. The **Full Server Backup** of your Windows 2008 Server using Windows Server Backup has now been successfully completed.

Summary of Exam Objectives

Microsoft has included many interesting and useful updates and additions with the new Windows 2008 Server O/S. In this chapter we have explored some of the best points of the new offerings that relate to Storage, High Availability, and Recoverability, all important components of any Enterprise class operating system.

The ease of use and improved capabilities in the tools provided for Storage Management, as well as the Self Healing and Data Security capabilities contained within the internal workings of the storage systems themselves, are of critical importance to organizations looking to protect data from the omnipresent threats of failures and security intrusions.

The greatly improved capabilities of the High Availability solutions provide a welcome break to administrators that have long struggled with complicated and often uncooperative clustering solutions. The dramatic simplification of the cluster creation process, made all that much better by the new Cluster Validation Wizard, means that setting up and maintaining a Failover Cluster solution no longer needs to be a hair-pulling experience for all but, and sometimes even including, the most experienced administrators. The redesign of the Quorum, or Witness Disk Model as it is now called, has resulted in a high Availability product that finally may be called worthy of the label “high availability.” As well, improvements to the Geoclustering capabilities is a factor that is sure to capture the attention of organizations looking for better, cheaper, and easier to implement and maintain Disaster Recovery options.

In the area of recoverability, much remains the same in Windows 2008 with respect to functionality and methodology. What has changed is the tool that is provided to accomplish these tasks. Ultimately, a backup is a backup, and a restore is a restore, but the redesigned Windows Server Backup tool has been recreated with the intent to make these familiar tasks simpler, faster, and more reliable. While it does depart from some of the interfaces that have become familiar to many long-time users of the old NT Backup Utility, with a little bit of poking around and practice, the newly designed tool will no doubt become the preferred standard for most, if not all. In short, it’s different, but in a good way that will undoubtedly grow on people.

Exam Objectives Fast Track

Planning for Storage Requirements

- With Self Healing NTFS the sequence of events is that NTFS will detect any file corruption, and make an attempt to recover or repair any such files.

If recovery or repair proves not to be possible, then the file will be deleted, and the event will be recorded in the Event Log.

- Self Healing NTFS can recover a volume when the boot sector is readable, but the NTFS Volume is not.
- When turned off, **Self Healing NTFS** will generate an alert when file corruption is detected, but it will not take action to correct it. In this case, the onus is on administrators to manually act upon the corruption warning using available tools
- Multipath I/O has been included as an optional feature with Windows 2008 with the intent to support failover redundancy and load balancing solutions. Multipath I/O provides support for iSCSI, Fiber, and SAN technologies.
- The options for Multipath I/O Load Balancing Modes of operation are, Failover, Failback, Round Robin, Round Robin with a subset of paths, Dynamic Least Queue Depth, and Weighted Path.
- The default configuration is Round Robin when the storage controller is set for active / active. When the storage controller is set for Asymmetric Logical Unit Access” the default configuration is Failover.
- Microsoft included the **Devices: Allowed to Format or Eject Removable Media** group policy object in Windows 2008 to allow administrators the option to prevent the use of specific types of removable media on servers.
- BitLocker Drive Encryption** is a new feature included with Windows 2008 that is designed to protect the Operating System and all data stored on the system volume from malicious activity. By default it only covers data stored on the system volume, but it can easily be configured to cover other volumes as well.

Data Collaboration

- There are two levels of Sharepoint services that are available to be deployed on the Windows 2008 Server platform. Windows Sharepoint Services 3.0 SP1 (WSS 3.0 SP1), and Microsoft Office Sharepoint Server 2007 (MOSS 2007)
- WSS 3.0 is a prerequisite to the installation of MOSS 2007. Any attempt to install MOSS 2007 without WSS 3.0 SP1 preinstalled will fail.

- WSS 3.0 cannot be deployed on a Server Core installation of Windows 2008 Server, as many of the needed prerequisites are not available on a Server Core installation. WSS 3.0 deployment is therefore only supported on a Full Installation of Windows 2008 Server.
- To successfully install WSS 3.0 on a Windows 2008 Server platform, you need to install a number of prerequisite Server Roles and features in advance. If you do not satisfy all of these prerequisites before installing WSS 3.0, the installation will fail.
- Server Roles—the Web Server Role
 - Windows Process Activation Service (WPAS): **Process Model, Configuration API, .NET Environment**
- Server Features—the .NET Framework 3.0
 - Role Services: **Application Development | .NET Extensibility, Windows Process Activation Service | .NET Environment**
- The deployment of the WSS 3.0 Server Role via installation using an executable file is an exception to the normal Windows 2008 Server method of Role deployment where such items are simply selected under the **Add Roles Wizard** and installed on an as desired basis. According to Microsoft, it is their intent to maintain the deployment of the WSS 3.0 Role in this format for the foreseeable future.

Planning for High Availability

- Failover Clustering has been dramatically improved in Windows 2008. The new features and functionalities offered with Windows 2008 clustering have been targeted at the areas of, Simplification, Improved Stability, and Improved Security.
- One of the most notable improvements to Failover Clustering functionality in Windows 2008 is the redesigned capabilities and functionality of the Quorum, now called the *Witness Disk*. The Witness Disk can now be configured in a manner that will allow the cluster to survive its loss in the event of a failure.
- In Windows 2008 the most desirable features and functions have been combined to create the **Majority Quorum Model**. In the Majority Quorum Model a vote system has been implemented, in order to assign a

value to each copy of the cluster registry files. Specifically, each node and the Witness Disk itself are assigned one vote, and as long as the majority of votes are online and available, so will the cluster.

- The way this works is that the disk on each node of the cluster that runs a copy of the key quorum registry files gets a vote. As well, the Quorum itself gets a vote since it is also obviously supporting a copy of these same key files. As long as the majority of votes are online and available, then the cluster will continue to run. This is made possible by the fact that a copy of the Quorum or Witness Disk contents are maintained on the local drives of each Node, as well as on the Witness Disk itself. Therefore losing a node or losing the Witness Disk are effectively the same. It's just one copy out of three available copies that will have been lost. The two copies that remain online and available represent the Majority of the available copies.
- In Windows 2003 Server the maximum delay that the heartbeat would tolerate before detecting a node failure was 500 milliseconds. By making the heartbeat delay wait time configurable to essentially any value in Windows 2008 Server the limitation on distance and connection speed between cluster nodes has been effectively eliminated. This means that cluster nodes can reside in different cities, or even different countries, without issue.
- In Windows 2008 Failover Clustering the nodes can be configured to exist on different subnets. This feature is also designed to support the ability to have geographically displaced nodes without the need to trick the cluster using VLANs.
- The addition of the Hyper-V Virtualization solution in Windows 2008 Server has allowed for a new way to use Failover Clustering to accomplish High Availability solutions. Windows 2008 Servers configured for the Hyper-V Role can now be configured as nodes in a failover cluster. This configuration allows for the Child Partitions containing the Virtual Machines to be hosted on a share storage platform that is equally available to each host. At any one time, only one of the cluster nodes will actually host the running VMs in an Active Passive mode configuration. This allows for the use of Hyper-V's Quick Migration functionality, where running VMs can be migrated from one host Node to the other without the requirement to be shut down.

Planning for Backup and Recovery

- Windows Server Backup uses Volume Shadow Copy Services (VSS) to accomplish its function, and backs up to the VHD File format. It can be used either for individual object, full volume, or full server recovery, called a *Bare Metal Restore*:
- The Windows Server Backup Utility provided with Windows 2008 Server does not support “Backup to Tape” functionality
- The Windows Server Backup Utility takes only one full snapshot of a volume. After that it’s just differentials.
- The selected local drive to which the backup file is to be copied must not be the same drive from which files are being backed up. Any attempt to back files up, and copy them to the same drive from which they are being backed up, will be met with an error message
- Windows 2008 Server has been designed to concentrate on the backup of “Critical Volumes” for the security of important files, and functionality
- The Windows Server Backup Utility provided with Windows 2008 Server does support “Restore” via the mounting of a VHD file.

Exam Objectives Frequently Asked Questions

Q: I have a server that is used exclusively for the personal working data of the executives within my organization. They have expressed the concern that this data is of an extra sensitive nature, containing important company secrets, etc. They have asked me to devise a solution that will guarantee that this data will not fall into the wrong hands, even after the server has been decommissioned. How can you accomplish this, in a way that will satisfy their concerns completely?

A: One of the methods available as a solution for this requirement is to employ BitLocker Drive Security to guarantee that anyone trying to steal a copy of this important data by pulling one drive out of the mirrored set on the server, or any other such measures, will find that they have stolen a drive that will not work on any other server. Without BitLocker decryption capabilities, the would-be thief will not be able to access anything on the drive. This also holds true for when the server is decommissioned.

Q: In my company, there is a concern regarding the ability for anyone to copy Virtual Machine Files from any of the domain controllers in our Lab environment onto the newer large capacity memory key devices available now. Such a person could then leave the company undetected with these files. Possibly contractors, or someone like this who comes and goes frequently, could be paid to acquire this information by our competitors, with the intent of corporate spying, sabotage, etc. How can we protect ourselves from this security threat?

A: By utilizing the Group Policy setting called **Devices: Allowed to Format or Eject Removable Media** you could effectively prevent the use of these memory keys, both in your lab environment, as well as in production. This would block any efforts by such persons with malicious intent from copying and stealing the virtual server files containing your Active Directory Database, as well as any other such files that are deemed to be of critical importance to your organization. As an added layer of protection for files of this nature, Auditing could be enabled to track and record file access attempts. With this feature enabled anyone attempting to copy the subject files would leave an audit trail that could be followed. To take it one step farther, System Center Operations Manager can be configured to generate alerts, and even page administrators when such a critical file copy action has been attempted.

With these measures in place, any would-be data thief would find it significantly more difficult to carry out such an act anonymously.

Q: I have a significant number of people asking me how they can effectively share data amongst coworkers both within their own departments, as well as interdepartmentally, in a safe, secure, and easily controllable manner. How can I do this without using standard file shares technology that might turn into an administrative nightmare, not to mention a security risk?

A: Plan and deploy Windows Sharepoint Services in your organization. I strongly suggest that the planning part of the equation not be ignored, otherwise you may find that the proliferation of Sharepoint sites within the organization may quickly get out of control, as each department discovers its advantages, and rushes to deploy their own individual solutions. This could quickly become a source of significant waste of not only administrative effort, but also of power and equipment.

Q: My organization is eager to deploy the new Hyper-V solution offered with Windows Server 2008, but we are worried about potential problems with the level of availability of these virtual assets once deployed. After all, with many virtual machines running on one host, this means that every time this one host requires maintenance of any kind which requires down time, we will simultaneously be affecting every virtual server hosted running on that host. How can I mitigate the effects of maintenance requirements to the servers hosting virtual machines on a Windows 2008 Hyper-V platform?

A: The answer is to deploy your Hyper-V solution in concert with Windows 2008 Failover Clustering solution. In this configuration, the Hyper-V hosts can be set up as nodes in a Windows 2008 Failover Cluster, allowing for the utilization of Quick Migration Technology. Quick Migration will allow you to migrate the Virtual Machines from one host to another within the Cluster, with only a minimal amount of down time. This down time will usually only amount to about 5 to 30 seconds, depending upon the class of hardware on which it is running, and the amount of available memory. While the quick migration of VMs from one host to the other does result in a momentary outage, it is still a viable option for workloads that can tolerate this short outage. And it will allow for the maintenance to any of the member nodes, without any other interference with the operation and availability of the guest VMs.

Q: My company is greatly concerned, not only about the high cost of maintaining our current disaster recovery solution, but also about the unacceptably long

period of time that has been demonstrated to be required to implement the solution during our bi-annual disaster recovery tests. The recovery of all critical server workloads from tape, as well as the synchronization of other critical resources as demonstrated during our DR testing, takes a long enough period of time that there is significant concern from management regarding the potential financial impact in the event that we ever had to actually put this plan into action due to some unforeseen event. How can I reduce these costs, as well as improve the recovery times in order to mitigate the potential effects of my organization's ability to conduct business in the wake of any real disaster, should one ever occur?

A: The new developments with respect to Geographically Disbursed Clustering are a perfect fit for this requirement. While it is true that not all workloads may be suited to the use of a clustering solution, it is certainly true that anything critical enough to be placed high on the list of items to be included in any DR solution are most likely also critical enough to consider for deployment on a Failover Clustering platform. Over and above critical business applications which may include E-Commerce Websites that generate revenue, and so forth, are the core network infrastructure services such as DHCP, DNS, DFS, and Printing capabilities, to mention just a few. These services can be clustered between sites using Windows 2008, in a manner that could provide an instant recovery capability in the wake of any sort of unforeseen event. In fact it could be possible that with proper planning and deployment many users at geographically dispersed locations may be left unaware that anything had even happened, in the wake of a loss of primary services at any particular site. This is possible with Geographically Disbursed Clusters on the Windows 2008 Platform.

Q: I have a need to regularly backup the Directory Services Database in my organization, but I want to be able to automate the process, and have it run in the background each evening. What is the best way to do this?

A: There is more than one way to accomplish this automated backup requirement. The best method depends heavily upon what the individual capabilities of the administrator implementing the solution are. For an administrator who is comfortable at the command line using PowerShell, the verbose functionality and control offered by PowerShell would most likely be the best way. However for an administrator who is new to PowerShell, and possibly needing more training to become comfortable with its use, then Windows Server Backup provides a perfectly acceptable version of this same capability that can be scheduled to run when and as desired.

Self Test

1. The Self Healing NTFS feature of Windows 2008 data storage can recover a volume under which of the following conditions? (Choose all that apply)
 - A. The server cannot be started
 - B. There is corrupt Data on the Volume
 - C. The Volume is unreadable.
 - D. The Boot Sector is unreadable.
2. What will occur in the event that Self Healing NTFS is unable to recover an individual file that has become corrupted?
 - A. A message will be displayed on the screen, warning the user about what has happened.
 - B. The file will be deleted.
 - C. The file will be moved to a quarantine folder to allow for efforts to recover it.
 - D. The file will be moved to the Recycle Bin where the user can choose to keep, or discard it.
3. Self Healing NTFS can be turned off by administrators who choose to do so. How will Self Healing NTFS behave when confronted with a corrupted file while its functionality is turned off?
 - A. It will still delete the file, but will not generate the event in the event log.
 - B. It will do nothing, as it is turned off, and therefore cannot function in any way.
 - C. It will generate the event in the event log, but take no action on the corrupted file.
 - D. It will try to recover the file, but then take no more action if unable to recover it.
4. Multipath I/O is designed to support which of the following storage technologies? (Choose all that apply)
 - A. iSCSI
 - B. Fiber
 - C. iSNS
 - D. SMB File Share

5. When a storage controller is configured to use Multipath I/O in the Active / Active configuration the default configuration for Multipath I/O Load Balancing is which of the following?
 - A. Failback
 - B. Failover
 - C. Weighted Path
 - D. Round Robin
6. What would be the most effective way to prevent security violations and data theft in a Laboratory environment? (Choose all that apply)
 - A. Configure the BitLocker Drive Encryption Group Policy to encrypt all data stored on Laboratory server data volumes.
 - B. Deploy all Laboratory Servers of the Windows 2008 Server platform. Since BitLocker Drive Encryption is a built-in function with Windows 2008, it will protect all drives automatically by default.
 - C. Install the BitLocker Drive Encryption Role on all Laboratory Servers and configure it to encrypt all data stored on Laboratory server data volumes.
 - D. Configure the **Devices: Allowed to Format or Eject Removable Media** Group Policy to prohibit the use of removable media devices in the Lab environment.
7. By default, when installed and enabled, BitLocker Drive Encryption is designed to encrypt which of the following files? (Choose all that apply)
 - A. Paging files
 - B. Hibernation Files
 - C. All data on all volumes contained on the server
 - D. Only the volumes that have been explicitly configured during installation to be covered by BitLocker Drive Encryption.
8. BitLocker requires the assistance of TPM hardware support to provide complete protection for system files. It can however be configured to work on hardware that does not support the TPM standard. In this configuration, there will be some files that BitLocker Drive Encryption will not be able to protect. Which of the following will not be covered by BitLocker Driver Encryption when deployed and configured on non-TPM supported hardware? (Choose all that apply.)

- A. Paging Files
 - B. The Master Boot Record
 - C. The BIOS
 - D. Hibernation files
9. In order to deploy a Microsoft Office Share Point Server 2007 solution on a Windows 2008 Server platform, which of the following prerequisites must be met? (Choose all that apply.)
- A. The Web Services optional server Role must be installed using Server Manager's **Add Features Wizard**.
 - B. WSS 3.0 SP1 optional server feature must be installed.
 - C. The Windows Process Activation Service must be installed.
 - D. The .NET Framework 3.0 optional server feature must be installed using Server Manager's **Add Features Wizard**.
10. Which of the following is the method used for the deployment of Windows Sharepoint Services 3.0 SP1 on a Windows 2008 Server platform?
- A. The WSS 3.0 SP1 optional server Role must be installed using Server Manager's **Add Features Wizard**.
 - B. The WSS 3.0 SP1 optional server Role must be installed using Server Manager's **Add Roles Wizard**.
 - C. The WSS 3.0 SP1 optional server Role must be downloaded in the form of an executable file.
 - D. The WSS 3.0 SP1 optional server feature must be installed using Server Manager's **Add Features Wizard**.

Self Test Quick Answer Key

- | | |
|----------------|----------------|
| 1. B, C | 6. D |
| 2. B | 7. A, B |
| 3. C | 8. B, C |
| 4. A, B | 9. C, D |
| 5. B | 10. C |

Chapter 10

MCITP Exam 647

Software Updates and Compliance Management

Exam objectives in this chapter:

- Patch Management
- Windows Server Update Services
- Security Baselines
- Using the GPO Accelerator Tool
- Using the Baseline Security Analyzer
- System Health Models

Exam objectives review:

- Summary of Exam Objectives
- Exam Objectives Fast Track
- Exam Objectives Frequently Asked Questions
- Self Test
- Self Test Quick Answer Key

Introduction

A number of jobs fall under the heading of Network Administration, but few are as important as keeping your servers and workstations updated with the latest software and in line with corporate standards. In its most simplistic view, Patch and Compliance Management is the practice of keeping your computers up-to-date with the most current updates to the operating system.

Unfortunately, the picture is not so simple. The number of applications that a network supports can be huge and vendors are constantly releasing new patches to address different types of problems. Security threats evolve quickly, patches can often interact, and sometimes patches are problematic or even have updates themselves. On top of this complexity is the need to manage your environment as a whole to control the patches that are deployed and to ensure your environment is maintained as a single enterprise platform. Clearly, a better way to control and manage patching in a networked environment is needed.

More than just making sure all of your machines are up-to-date, it is crucial that a single corporate standard be maintained across the entire server and workstation inventory. This limits the complexity involved in maintaining your environment and helps protect from outages and inconsistencies that can arise as different versions of applications interact and work together to solve business problems. Ensuring your machines comply with update and security standards is important so problems can be swiftly resolved before they have a chance to really impact the network.

Managing updates and upgrading a network environment is not a new problem and has been one of the core duties of the network administrator since networks first began to enter the business sector. In companies that were not large enough to need a staff dedicated to maintaining a mainframe, these duties were often assigned to a lucky few who were volunteered from back office departments to support these new support roles. Quickly though, the scope and complexity of maintaining the servers and workstations became a full-time job requiring expertise and specialization.

Until recent years, patch and compliance management had not been a core part of the operating system. Individual products were tracked for updates and these were applied one at a time as they became available. More complicated still was that many of these relied on common libraries or operating system components, causing them to occasionally interact and conflict. A number of products have existed in the market to address true enterprise patching across all vendors and applications, but these are often complicated and hard to deploy.

Rather than relying on a patch and compliance management system that tries to accommodate applications across all vendors, Microsoft has introduced a number

of tools that can be used to update, audit, and monitor the core Windows operating system, productivity suites, and server products. These products fall into three broad categories.

- **Patch Management** This is the broad management of system updates, drivers, and security fixes that are managed and deployed in an environment.
- **Security Baselines** In order to maintain security and ensure there are no unmitigated security holes in your environment, it is important to audit and review your configurations periodically to provide a clear picture of the network as evaluated against industry best practices.
- **Health Modeling** In order to manage the health of a system in a holistic manner, it is important to look at system health in light of business function and the fitness of a workstation to participate on the network against predefined criteria.

NOTE

An enterprise health management plan will use all three of these different techniques to comprehensively manage all aspects of the environment. Any one of these in isolation can deal with specific problems, but when combined, they can prevent many of the headaches that may plague an environment. These become especially important as more services are incorporated into your environment that rely on assertions of system health to determine network access. Without these, technologies like Network Access Protection (NAP) become difficult to manage.

Value Proposition

Patch and compliance management is an easy thing to ignore or put off as the value it brings is in the prevention of problems and the mitigation of risk to the business. Like antivirus or backups, patch management shows its value in every day that something *doesn't* happen. For this reason, it is difficult to measure the return on investment without looking at a broader view of your environment.

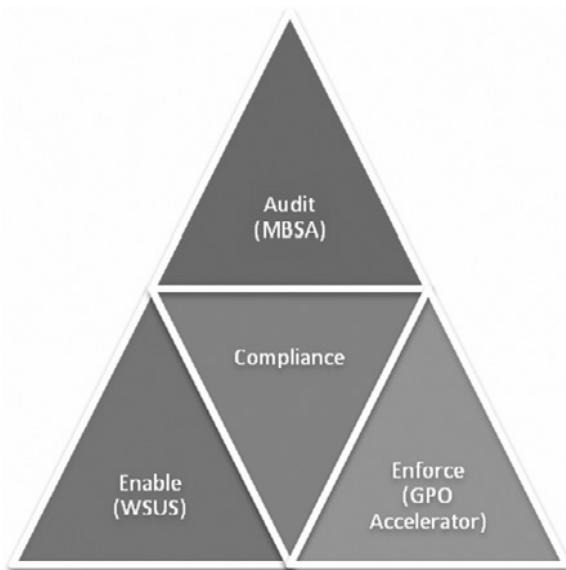
As a relative cost, it is easy to show that well-planned automated patch management is more cost-effective than approaching it as a manual process only to be done when a specific need arises. The configuration of a management scheme is relatively

simple and uses few resources to maintain and set up. The biggest win here is in the centralization of the management to a single point rather than having to access and configure each machine on your network. Further, there is a reduction of stress on your network as downloads of patches are centralized rather than having all workstations individually retrieve their updates.

The Compliance Picture

Three primary dynamics should be considered when evaluating the overall compliance of your client machines or network against your corporate security policy. It is important to be able to manage the ability of your environment to comply with the security standards you have set forth. Compliance is a multifaceted relationship balancing different business objectives that support the overall IT need for accountability against the need for systems that are easy to adopt (Figure 10.1).

Figure 10.1 The Compliance Triangle



- **Audit** You must periodically audit your environment to ensure that policies, security configurations, and updates are being distributed to client machines as expected.
- **Enable** Services must be made available to machines in your environment that can provide updates and resources to help bring them into compliance

with the security policies. This is especially important where NAP has been deployed to only grant network access to machines that meet specific health criteria.

- **Enforce** Enforcement of Security Policies and corporate standards must be done to protect the network and mitigate operational risk.

Patch Management

In managing the patches across your environment, it is important to consider the network as a whole. Maintaining the patch levels is more than just making sure the operating system is up-to-date. Individual applications, component drivers, the workstation BIOS, and their subsystems all need to be updated to protect the workstation and provide optimal performance.

Some risk is inherent in making changes to the core operating system or the system applications. For this reason, it is important to take a careful planned approach to system patching (Figure 10.2). While software and hardware vendors do extensive testing before a patch is released, occasionally a patch will be released that introduces other problems into your network. Most often, this is due to interactions with other software and configuration choices existing in the environment.

Figure 10.2 The Patch Management Process



Most network administrators will build a test lab where patches can be tested in isolation so that any negative effects can be discovered before a wider deployment is attempted. In highly structured environments where system configurations are controlled through the use of images and desktop management software, the test environment will consist of a specimen of each major configuration or image in production. This provides a high level of availability for the environments as it allows patch management to be done quickly and efficiently while reducing the overall risk that a single change will negatively impact the workstations and servers.

In addition to a test environment, it is important to identify a group of production users who are willing to participate in User Acceptance Testing (UAT) as a first wave of deployment before a set of patches becomes widely available. Once these users have received the patch and it can be verified that there are no adverse effects, the patch can be considered for full deployment to the production environment.

NOTE

It can be very tempting to use the IT department as the test environment for UAT—they are very understanding as you work through problems, you work directly with them, and you can avoid embarrassment should there be an issue. The downside is that these users are not representative of the users across your organization and can have configurations that are not indicative of the corporate standard. Furthermore, if there is an issue with the patch, the risk associated with the possibility of crippling the IT department is huge as the people responsible for resolving the issue might not have access to the tools they need to work in a crisis.

It is usually best to choose one or two machines from each major department to build that UAT group. Users in Accounts Receivable will have dramatically different system configurations than someone in Research and Development or Marketing. Choosing cross-functional groups helps to keep the whole organization involved in IT and can help identify problems quickly before there is an opportunity to completely shut down users across an entire department. As in anything like this, the value to the organization must be clearly articulated so each department is invested in protecting their function through participation in testing.

In defining the patch management strategy that you would like to deploy in your network, it is important to look at the risk you are willing to accept in your network. Anytime changes are made to the workstations and servers in your environment, a certain amount of risk is incurred. This should be carefully weighed against the risk posed by doing nothing. In the case of security updates and critical updates, these updates have been deployed to specifically counter known security holes and exploits in the wild.

OS Level Patch Management

Network environments are usually a complex and highly heterogeneous mix of different hardware and software all built to support the function of a business enabling its users to work together in a collaborative fashion. It is this heterogenic nature of networks that can lead to many of the challenges network administrators deal with

in the course of their jobs. Many of the differences in the hardware platforms can be mitigated through the common interfaces exposed by the operating system, but these too can lead to interoperability problems if they are not properly maintained.

For this reason it is important that the operating systems across the network are kept updated. This not only helps protect the environment from security exploits, viruses, and malware, but it forms a single cohesive platform on which the client applications can run.

Windows Server Update Services

The Windows Server Update Services (WSUS) is a vital tool for the network administrator running a Windows 2008 infrastructure as it forms a platform for centralized patch distribution and auditing. This product is available as a free download from Microsoft and is closely integrated with both the server and workstation operating systems relying on domain membership and group policy to control the updates that are pushed to the clients.

WSUS is able to provide more than just operating system updates, but can also control and maintain a number of core Microsoft applications on both the Server and workstation platforms, allowing the network administrator to use it as the core of a comprehensive patch management program. The following products have been updated with WSUS:

- Exchange 2007 Anti-spam
- Exchange 2000–2007
- Internet Explorer 7 & 8
- Internet Security and Acceleration Server (ISA) 2004 and 2006
- Microsoft Compute Cluster
- Microsoft Core XML Services
- Microsoft Expression
- Microsoft Forefront
- Microsoft ISA Firewall Client
- Microsoft Office 2002/ XP – 2007
- Microsoft SilverLight
- Microsoft SQL Server 2005
- Microsoft Virtual Server

- Network Monitor 3
- Office Communications Server (OCS) 2007
- System Center Data Protection Manager
- Systems Management Server (SMS) 2003 and 2007
- Visual Studio 2005
- Windows Live Applications
- Windows Server 2000, 2003, 2008
- Windows Small Business Server (SBS) 2003
- Windows 2000, XP,Vista

System Requirements

On the Windows Server 2008 platform, a number of components must be installed and configured to support the application. Disk space also must be made available for the WSUS Content Stores and the associated management database.

- Web Server (IIS) Role
- Security | Windows Authentication
- Application Development ASP.NET
- Management Tools | IIS 6 Management Compatibility
- Management Tools | IIS 6 Metabase Compatibility
- Microsoft Report Viewer 2005 Redistributable
- .NET Framework 2.0
- BITS 2.0
- SQL 2005 SP1 (If you are not planning to use the Windows Internal Database)

NOTE

The Background Intelligent Transfer service (BITS) 2.0 is a managed download service that allows for an asynchronous download of files after the service that initiated the download closed. This allows for a variable download speed that is able to respond to network conditions and connection contention. This allows the download of patches to happen in the background with only a limited impact on the client operation.

In addition to these component requirements, sufficient disk space must be available.

- **1GB System Partition** This space is used to store the operating files and Web instance to support WSUS and its services.
- **20GB Content Store** This is the space used to store the downloaded patches that are to be deployed to the client machines. When several languages are selected, additional space may be required. You should have at least 30GB if you are storing more than just English updates.
- **2GB Database Store** If you are planning to use the built-in Windows Internal Database, you should have at least this much space free. In larger environments, additional space might be required to support SQL Server 2005 SP1 as the datastore.

Types of Patches

A number of different patch classifications can be distributed through a WSUS server. While all of these may be important, they are not always appropriate for all situations as additional storage is required on the WSUS server to make them available, and inclusion of all of them can dramatically increase the approvals the administrator will have to wade through.

- **Critical Updates** These updates are the most critical to the security and function of the network environment since they are released to specifically deal with security and functional flaws found in Microsoft products. These will usually be in response to a vulnerability that is already in the wild and may already have known exploits.
- **Definition Updates** If you choose to update the Windows Defender application to control spyware, adware, and malware, you will have the option to deploy defender definitions through WSUS. These updates make the Windows Defender aware of new malware exploits and allow it to prevent infection and clean machines that have already been affected by the exploit.
- **Drivers** Updates to hardware drivers can be deployed through WSUS to provide enhancements to things like video cards, sound cards, network interface cards (NICs), communication subsystems, and other components.

NOTE

In practice, deploying driver updates through WSUS can be impractical as the number of hardware driver updates can be truly large, forcing you to sort through dozens of new updates every time you review your WSUS implementation. After doing this for a few weeks, many people start to ignore the Drivers category.

There is also some additional risk in deploying device drivers if you haven't built a sound testing environment. When hardware drivers become corrupt, it will often affect the overall operation of the machine rather than simply disrupt an application. This means that a malformed display driver could completely shut down an entire organization if it is not appropriately tested before deployment.

- **Feature Packs** New functionality that is deployed as an optional extension of an existing application is deployed in feature packs. These have traditionally been rare, but provide significant extension of the core product.
- **Security Updates** These confer enhancements in the security of the patched applications. They generally improve the security of current products rather than addressing new security holes with known exploits.
- **Service Packs** As the operating systems and applications evolve, major jumps forward in the functionality and feature set are deployed in service packs. Traditionally these have been difficult to deploy and require the most extensive testing due to the number of changes bundled in the update. Special care should be taken to preserve the testing process with service packs and to ensure that deployments are done in a controlled manner.
- **Tools** These are additional management and administrative tools that can be helpful for network administrators and power users. These are not essential to the function of the network, but can often provide additional functionality and give a better user experience.
- **Update Rollups** Periodically, a large number of updates will be bundled into an Update Rollup that will allow new workstations to apply many updates in a single shot rather than doing them one at a time.

This provides a more convenient path for network administrators, especially if patches are done more infrequently, as leaps forward rather than a gradual evolution.

- **Updates** These are periodic updates to the windows operating system and core Microsoft applications that provide additional security or resolve specific functionality deficits in the product. These are traditionally released on the second Tuesday of the month, though they can be released at any time. These differ from Critical Updates in that not applying these does not usually result in an imminent threat to the security of the application or corporate data. These should be taken seriously, however, as they are important to the maintenance and function of the network.

Comparison to Microsoft Update

Microsoft Update is a cursory patch management solution made available through the Microsoft Web site and is the foundation on which both WSUS and the MBSA are built. Windows Update maintains a database of Microsoft applications and operating systems, along with the associated patches available with each. When a workstation attaches to Windows Update, the current patch level for each of the managed applications is compared against the patch database so any outstanding patches can be identified. At that point, the appropriate patches can be downloaded and applied.

This process works well for very small environments or single home computers, but in larger enterprises it is an unattractive solution. It might be practical for a single machine to download a large update or hotfix, but when it is needed across hundreds or thousands of workstations, the bandwidth needed to download a new copy for each machine becomes a serious problem.

This also means there is no centralized control of the workstations, since each machine is responsible for maintaining its own updates. The users on each machine would have to have the elevated privileges required to download and install the updates. More challenging is the fact that some users would elect not to download or apply patches, thus opening the network up to attack and increasing the chances that corporate data might be compromised.

This lack of centralized control also means there is no enterprise-wide reporting. If you need to know if an individual patch has been applied to all machines in your environment, you would have to touch each machine, rely on third-party tools, or take your users' word for it. This isn't a reliable solution, especially for compliance auditing.

NOTE

Remember that Microsoft Update is primarily geared towards home users and small business that will not be significantly affected by individual downloads or the lack of centralized control. While almost any organization can benefit from the additional features of WSUS, its scalability and management capabilities are what give it real power.

Implementing WSUS

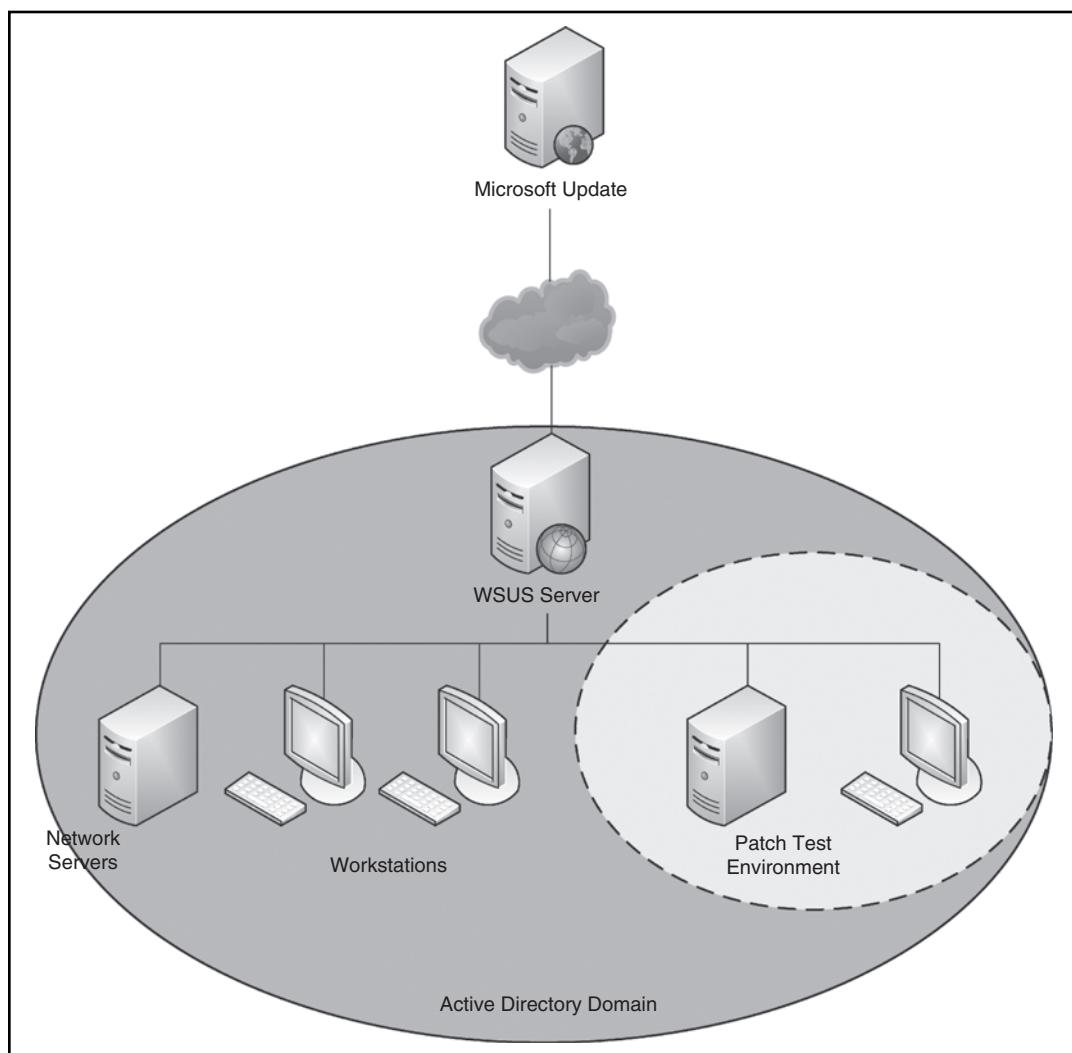
WSUS is an incredibly scalable tool that can provide operating system and core application patch management across a number of different physical network architectures, scaling from single server environments to truly large enterprises. In spite of the flexibility and scalability of the application, it is simple to deploy and manage, having been improved from earlier versions. A number of factors must be considered when designing a WSUS implementation.

Designing a WSUS Infrastructure

A high level of flexibility is built into Windows server update services that allow it to be configured to meet the needs of almost any infrastructure from a small single server shop to a truly large enterprise. Building on the strengths of the platform, a number of different configurations are possible to support these different scenarios, each providing solutions to specific challenges that are present in each scenario.

Small Enterprise (1–100 Workstations)

In the small enterprise, the focus is usually on providing services while minimizing cost and complexity for maintenance. In this configuration, a single WSUS server is responsible for pulling updates down from the Microsoft Update site and distributing them to all of the workstations and servers in the environment. This scenario also takes advantage of the Windows Internal Database for its storage solution (Figure 10.3).

Figure 10.3 WSUS in the Small Enterprise

This simplicity does come with the disadvantage of introducing a single point of failure to the system. In the smaller enterprise, this is not usually seen as a major hurdle since it is still feasible for the individual workstations to download the updates directly, should that be needed.

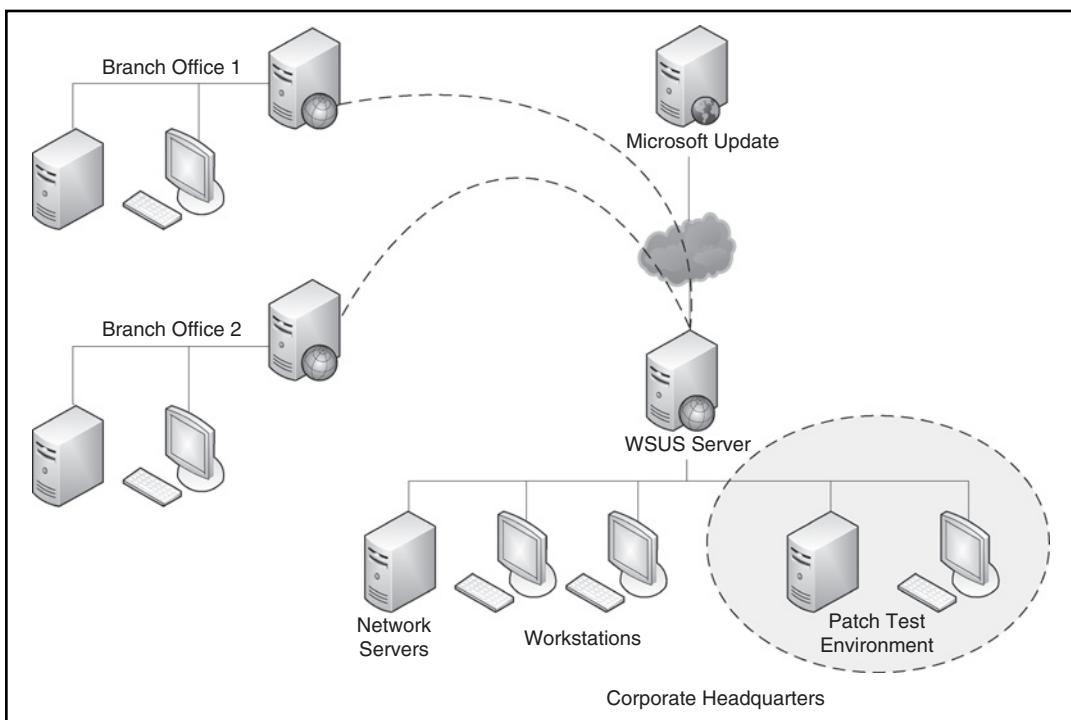
Branch Office Deployment

As an environment grows, it will often add additional sites rather than simply increase the number of workstations at a single location. These branch offices are usually

connected back to the core site by slower WAN links that should be used for routing corporate data and often voice traffic. Because of the competition between all of the traffic on the WAN links, it is important to minimize the traffic passed over this link and control the flow of data to minimize the negative impact on the business.

To support the branch office structure, subordinate WSUS servers can be deployed at each one of the additional offices to control the flow of traffic (Figure 10.4). In this scenario, the downstream servers will contact the main corporate WSUS server to get updates for the patch content, as well as to synchronize the database controlling the approval status of each of the patches. This allows the download of the patches to be minimized and scheduled while keeping the update traffic between the WSUS server and the workstations on the local segment. This protects the bandwidth between the branch office and the corporate headquarters while continuing to provide update services to the clients.

Figure 10.4 WSUS in Branch Office Deployment



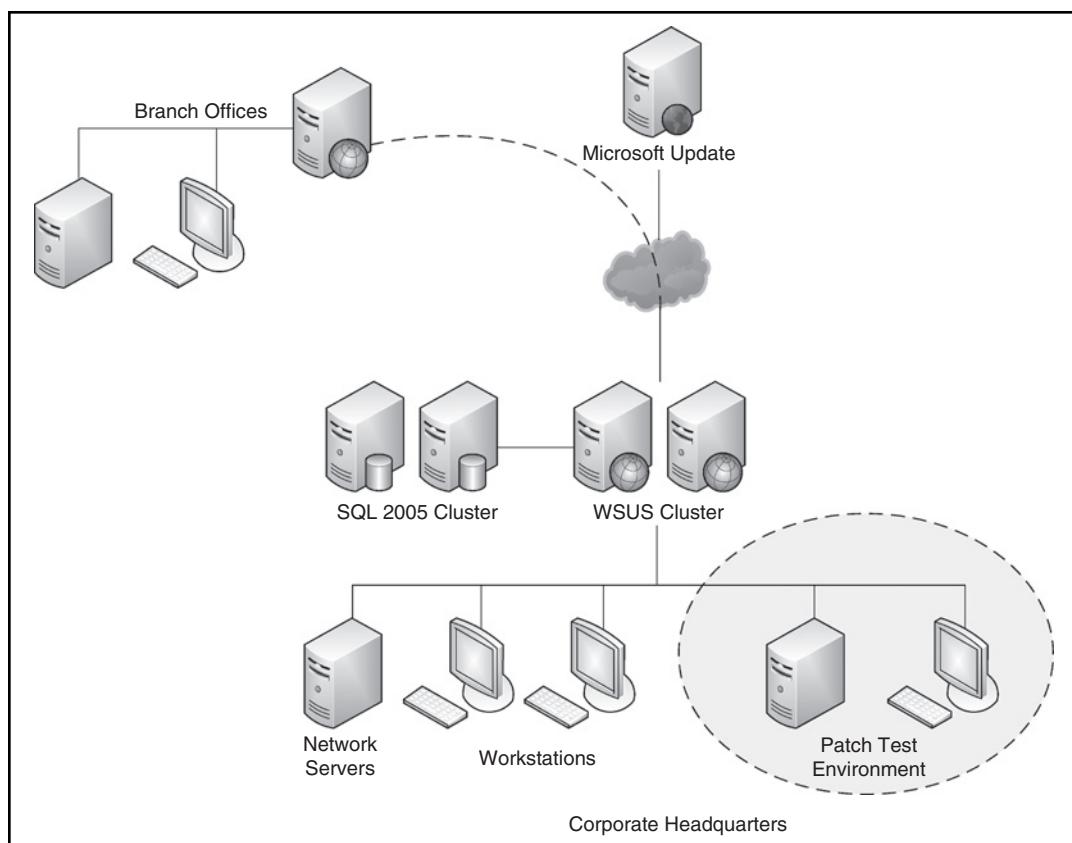
Large Enterprises

In the large enterprise, the primary focus is in maximizing system availability and building an environment that is able to scale well while continuing to provide service.

The IT infrastructure in larger organizations can range from highly developed organized systems to sprawling environments that have grown organically as business units and users have been added. Implementing WSUS in this kind of environment will require intimate knowledge of the environment and the links between sites. It is usually helpful to use the Active Directory topology as a guide when planning this kind of implementation since the site topology there will usually mirror the required WSUS structure.

In order to provide the required availability that large organizations need, WSUS can be clustered to ensure these services are always available (Figure 10.5). Additionally, the implementation of SQL 2005 as the database allows WSUS to serve a greater number of users supporting almost any level of complexity in the configuration and depth of group definition.

Figure 10.5 WSUS in the Enterprise



When you are implementing a WSUS infrastructure, it is important you understand your environment and choose the design that is most appropriate to your needs, cost sensitivity, and WAN topology. There is no single one-size-fits-all design, but rather a flexible platform that can support a number of different configurations and provide update services for nearly any environment.

In Exercise 10.1, we will be installing the Windows Server Update Services on a machine running Windows Server 2008 in a domain configuration with Windows Vista workstations participating in the domain. While configuring this environment is not covered in this script, every effort has been taken to keep the environment simple to avoid steps that do not directly support the exercise.

EXERCISE 10.1

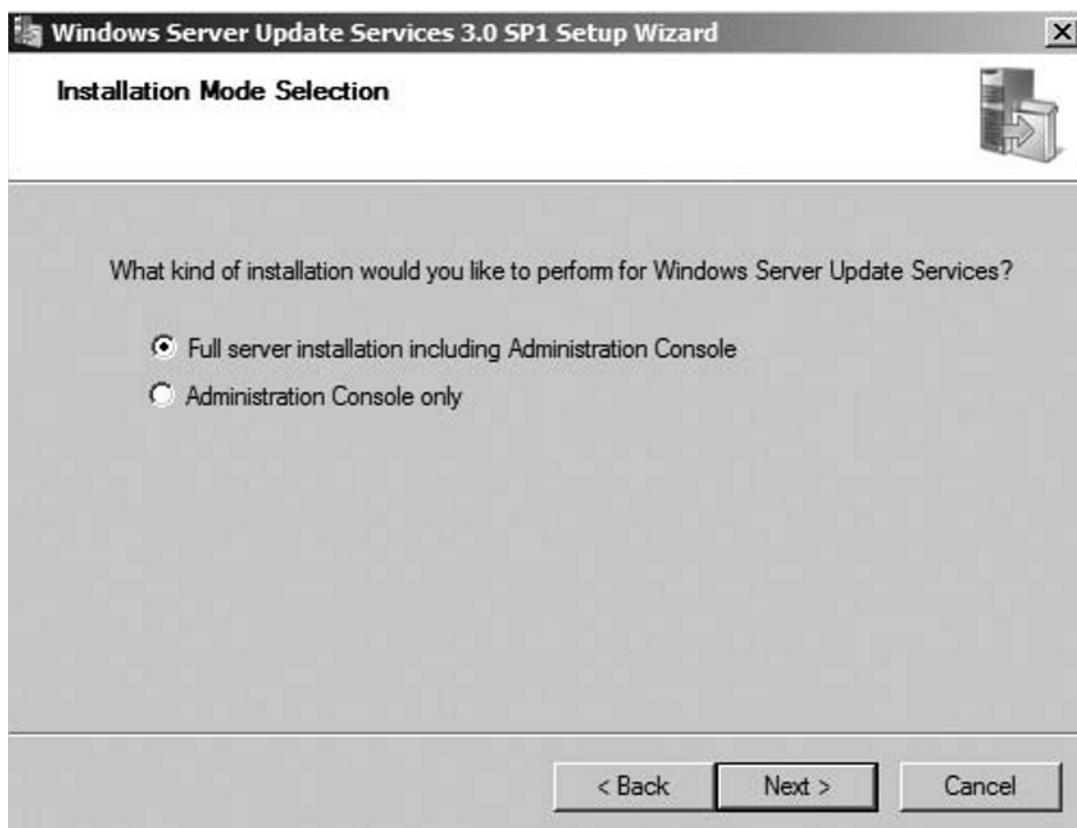
INSTALLING WINDOWS SERVER UPDATE SERVICES

1. Log on to the Windows 2008 machine with Administrator credentials.
2. Download the version of WSUS 3.0 SP1 from microsoft.com/download that is appropriate to your server's processor architecture (x86, x64, or IA64).
3. Double-click the downloaded application to begin the installation process.
4. On the Welcome screen, click **Next** to begin the installation (see Figure 10.6).

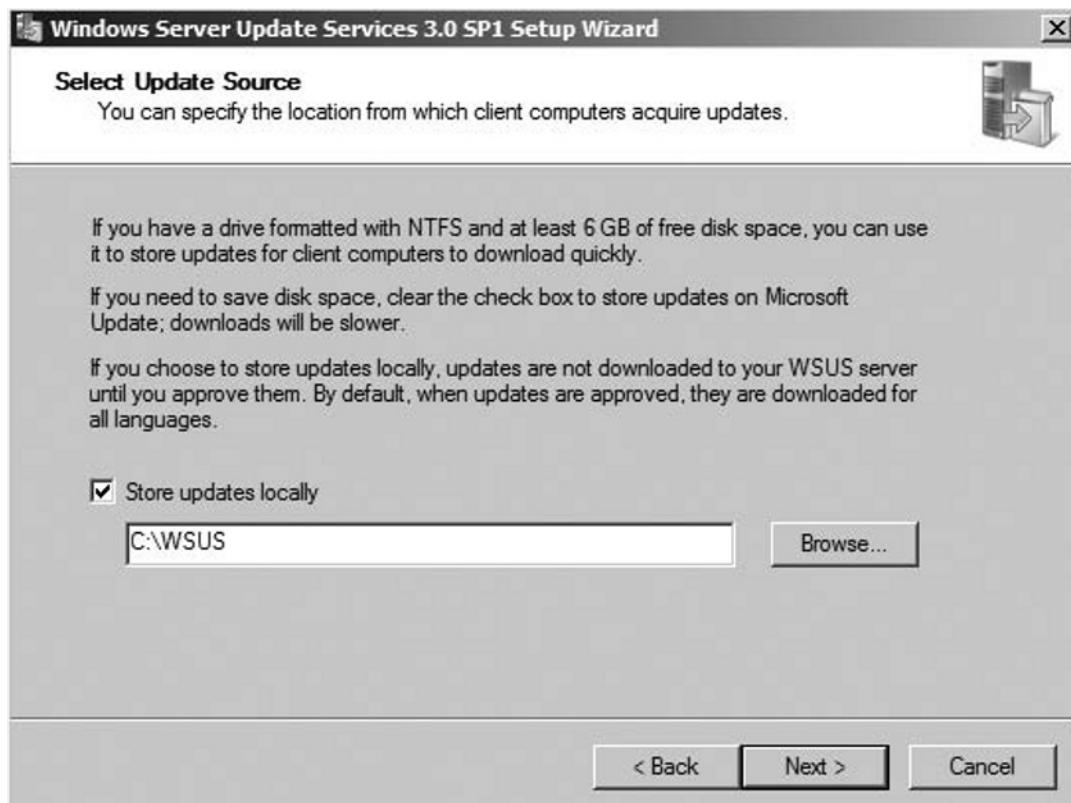
Figure 10.6 Installing Windows Server Update Services



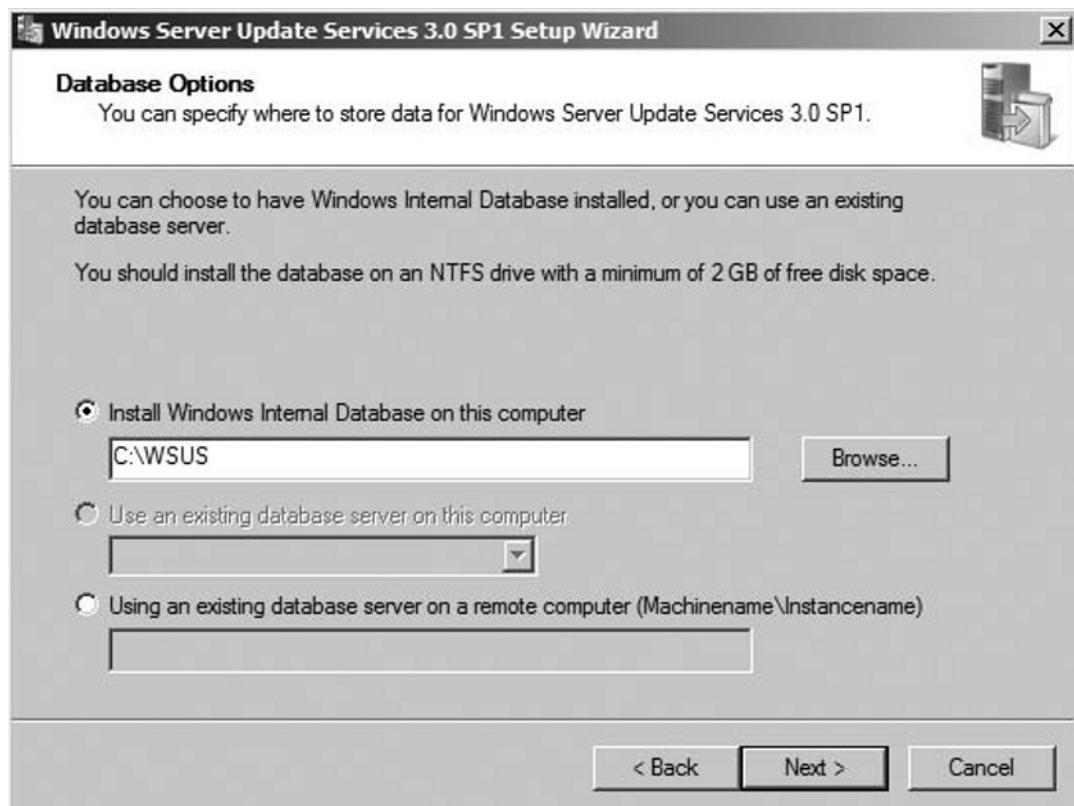
5. On the Installation Mode Selection screen, choose the radio button for **Full server installation including Administration Console** and click **Next** (see Figure 10.7).

Figure 10.7 Selecting a Full Server Installation

6. Accept the License Agreement and click **Next**.
7. If prompted that the Microsoft Report Viewer 2005 Redistributable is not installed, click **Next** to proceed. This can be installed later and will not affect the installation or configuration of WSUS in your environment.
8. On the Select Update Source screen, ensure that the Store Updates Locally box is checked and specify the path where you would like to store the updates for distribution (see Figure 10.8). Click **Next**.

Figure 10.8 Storing Updates

9. On the Database Option screen, choose **Install Windows Internal Database on this computer** to use the built-in WSUS database (see Figure 10.9). Alternatively, you could choose to deploy to an existing SQL 2005 SP2 instance, but this is not required outside of a production installation. Click **Next**.

Figure 10.9 Specifying Where to Store Your Data

10. On the Web Site Selection screen, select the radio button to use the IIS Default Web site. Make note of the Web address and port listed on the screen (see Figure 10.10). Click **Next**.

Figure 10.10 Selecting a Site to Use for WSUS Web Services



11. Review the settings that WSUS 3.0 will use to install and configure the services and then click **Next**.
12. Wait as the database is configured and the service is installed.
13. Click **Finish** to end the installation.

At this point, Windows Server Update Services has been installed on your server. You must now configure the server to download the appropriate updates from Microsoft and manage the pool of updatable servers and workstations on the network. This must be completed before the WSUS service is able to provide update services to your hosts.

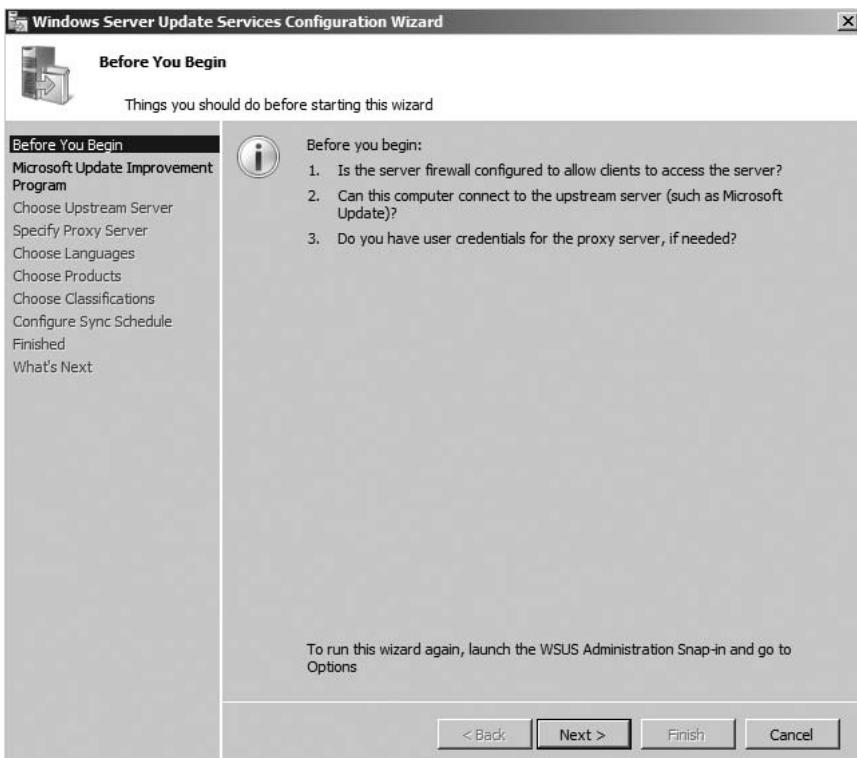
If you are continuing on from Exercise 10.1, you can proceed directly to step 5 of Exercise 10.2.

EXERCISE 10.2

CONFIGURING WINDOWS SERVER UPDATE SERVICES

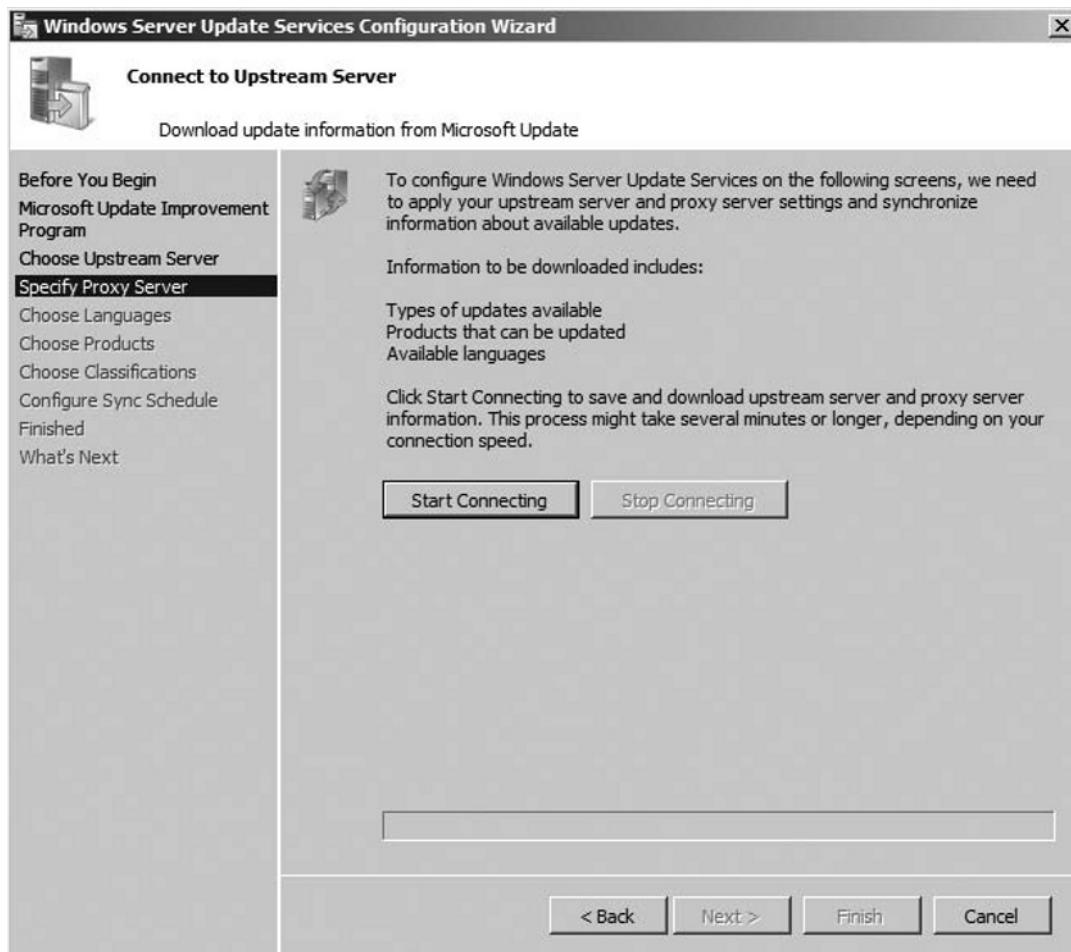
1. Log on to your Windows 2008 Server with Administrator privileges.
2. Navigate to **Start | Administrative Tools | Microsoft Windows Server Update Services 3.0 SP 1**.
3. Expand the server node on the left pane. Click **Options**.
4. In the center Options Pane, scroll down and choose the **WSUS Server Configuration Wizard**.
5. Review the warnings on the Before You Begin page and remediate any known issues (see Figure 10.11). Click **Next** to begin the configuration of the WSUS services.

Figure 10.11 Configuring Windows Server Update Services



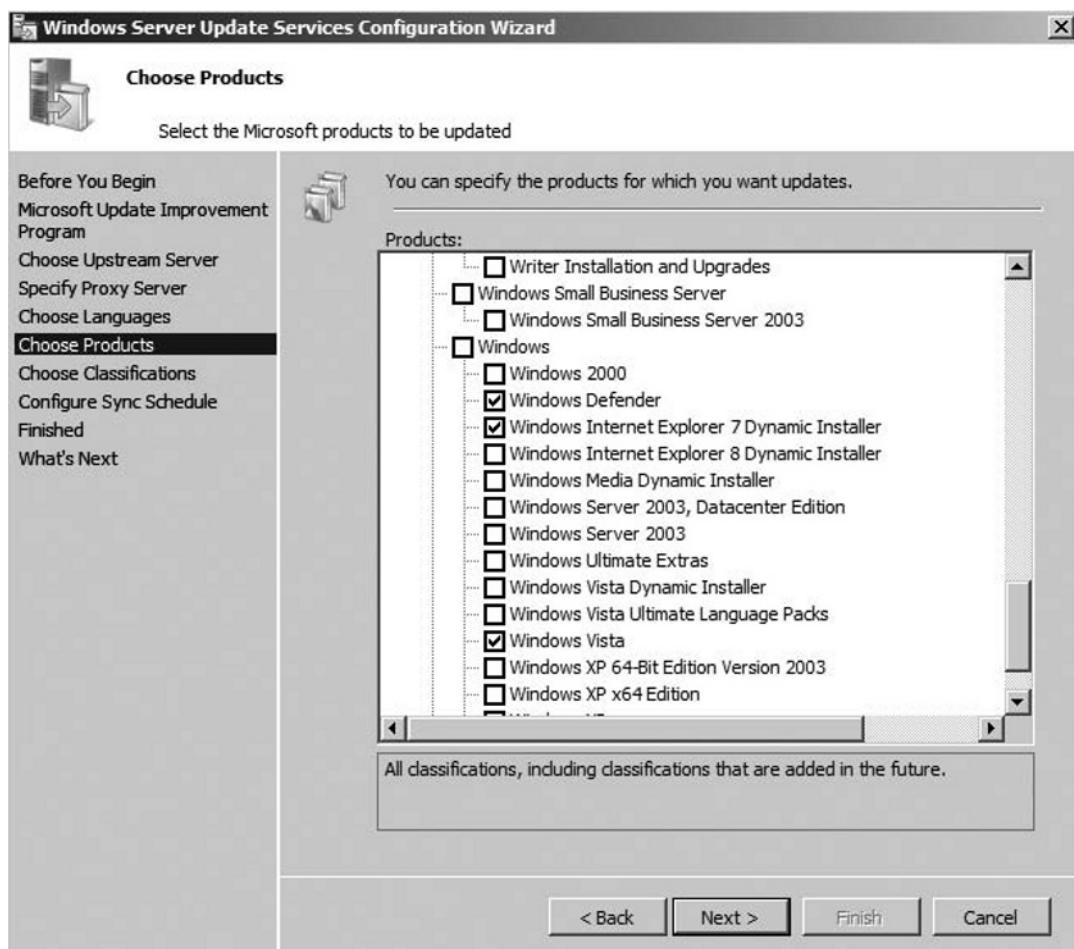
6. On the **Join The Microsoft Update Improvement Program** page, uncheck the box to join the program since this is not a production installation. Click **Next**.
7. On the **Choose Upstream Server** page, make sure the radio button for **Synchronize With Microsoft Update** is selected and click **Next**.
8. On the **Specify Proxy Server** page, click **Next**.
9. At this point, the server will need to connect to Microsoft Updates to download the catalog of available updates. Click **Start Connecting** and wait as the catalog is retrieved (see Figure 10.12).

Figure 10.12 The WSUS Configuration Wizard



10. Once the connection process is complete, click **Next**.
11. On the **Choose Languages** page, select **English** and click **Next**.
12. On the **Choose Products** screen (see Figure 10.13), select:
 - Windows Defender
 - Windows Internet Explorer 7 Dynamic Installer
 - Windows Vista
 - Windows Server 2008

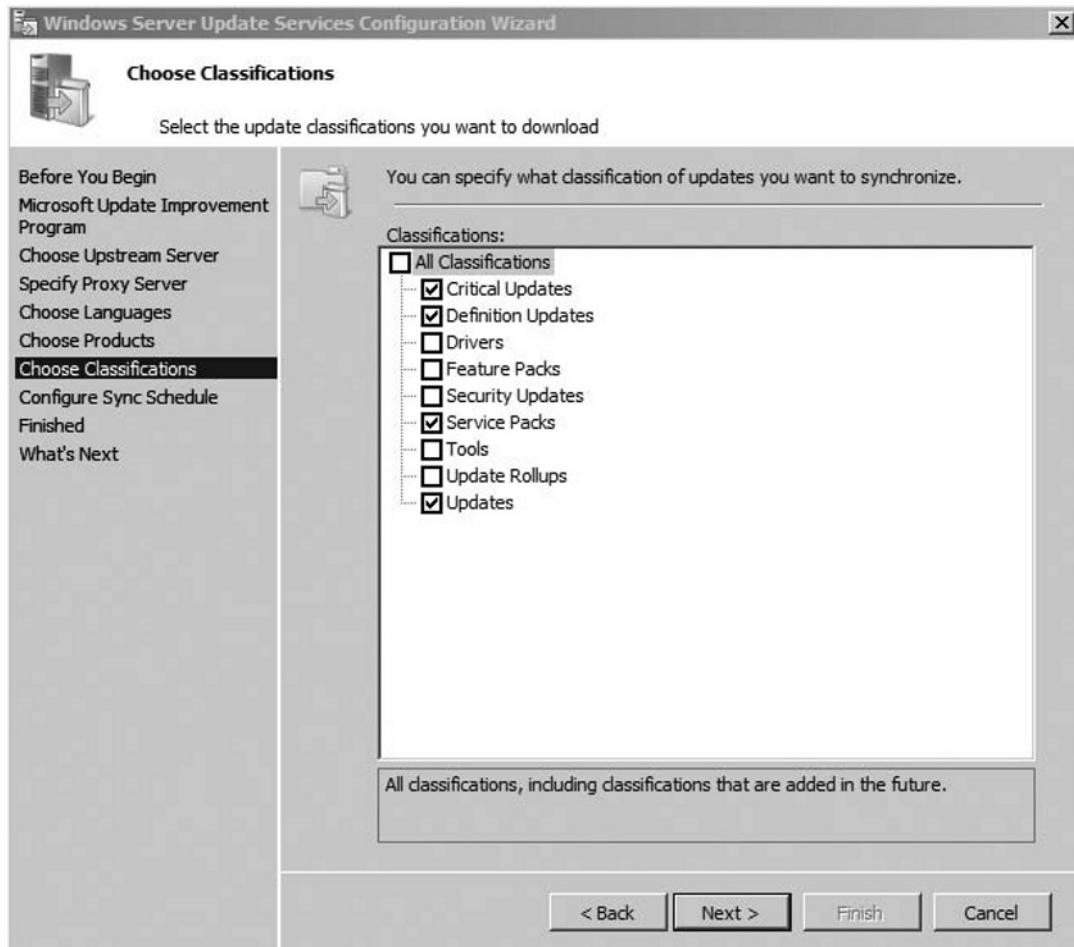
Figure 10.13 Selecting Products to Update



13. Click **Next** to continue the installation.

14. Select the classifications of updates you would like to make available through WSUS (see Figure 10.14):
- Critical Updates
 - Definition Updates
 - Service Packs
 - Updates

Figure 10.14 Selecting Classifications of Updates

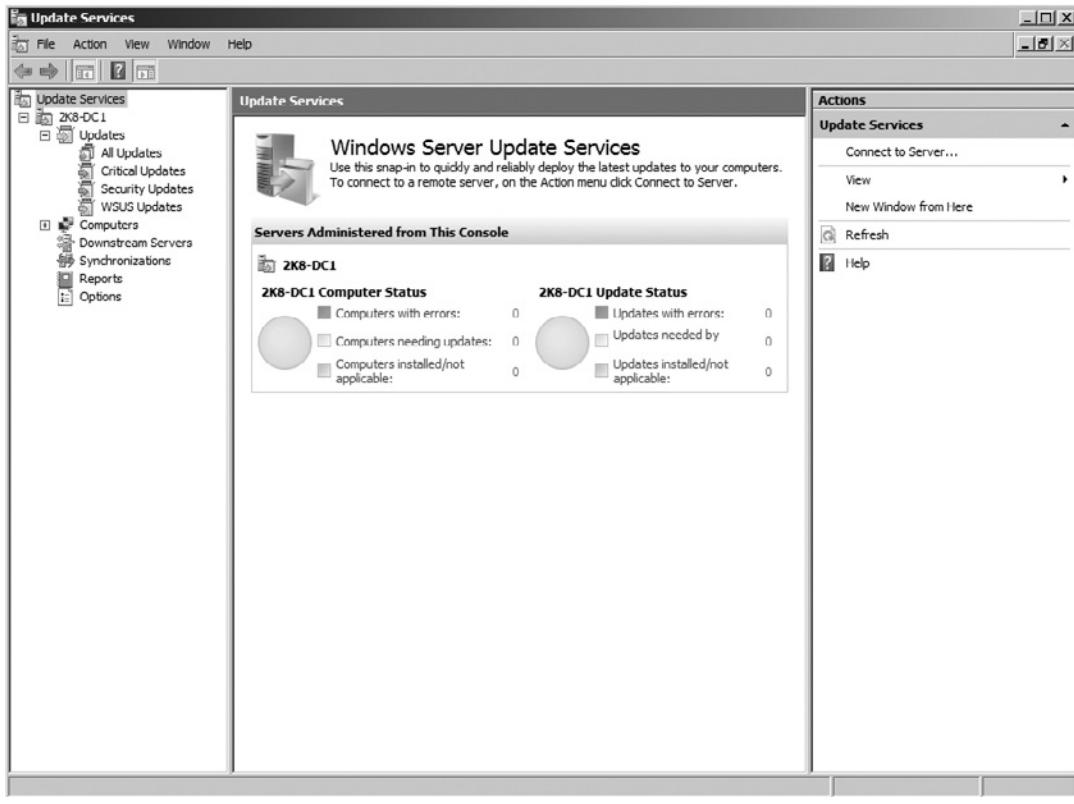


15. Click **Next** to continue the installation.
16. For this exercise, ensure that the radio button labeled **Synchronize Manually** is selected and click **Next** two times.

17. Click **Finish** to complete the installation.

At this point, the server will begin its synchronization process with Microsoft Updates, and the Update Services Role console will open to allow you to track and manage the operation of WSUS (see Figure 10.15).

Figure 10.15 The Update Services Role Console



Deploying to Client Computers

Once you have configured the server components of WSUS, you will need to configure the workstations and servers to use it as their update source. Otherwise, they will continue to contact Microsoft Update directly and will not benefit from your configuration. All machines that will use the WSUS server for updates must have a

compatible version of the Automatic Updates engine. The first time they contact the WSUS server, the workstations will be given an opportunity to update their engine. Workstations can use two methods to locate and connect to the WSUS servers.

- **Domain Group Policy** The best way to connect client machines to Windows Server Update Services is through a domain group policy. This allows the network administrator to control the deployment of updates and participation in the WSUS structure so it mirrors the structure of the active directory itself.
- **Local Group Policy** In environments that do not have Active Directory installed or that may have machines outside of the AD's control, connection to the WSUS servers should be done through local group policy. This allows the network administrator to specify the WSUS server to which the client should connect without requiring that the machine be subject to the larger GPO. This can be especially helpful for machines that are situated on a perimeter network, are outside of the domain, or are part of a foreign domain but attached to your infrastructure.

NOTE

Most network administrators are accustomed to working with Group Policy Objects (GPOs) but it is relatively rare that site policies will be used in the average network configuration. In an enterprise or branch office configuration, it is often helpful to deploy site policies to connect machines to WSUS servers that are local to them. This is especially helpful for laptops and mobile machines that are transient and will roam from site to site.

It is also generally a good idea to create a separate policy for the deployment of WSUS rather than including these settings in the Default Domain Policy. This gives you a finer level of control over the action of the GPO and will provide better flexibility as your environment grows. Implementing your policy this way will allow you to use GPO filtering through read and apply security rights to control the behavior and scope of effect to the clients. This needn't be a GPO completely dedicated to WSUS, but should be subordinate to the top-level policy.

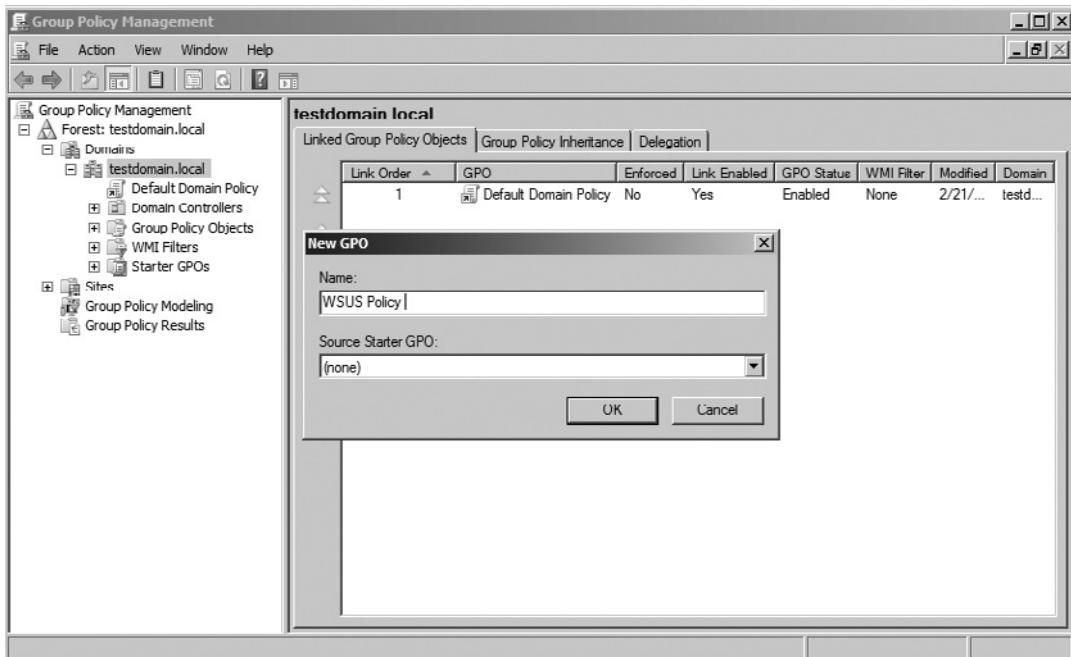
In Exercise 10.3, we show you how to configure WSUS clients.

EXERCISE 10.3

CONFIGURING WSUS CLIENTS

1. Log in to your domain with Administrator Credentials.
2. Navigate to **Start | Administrative Tools | Group Policy Management**.
3. In the right pane, expand the **Domains** node.
4. Right-click your domain and select **Create a GPO in this domain, and Link it here...**.
5. In the New GPO pop-up, enter **WSUS Policy** for the policy name and click **OK** (see Figure 10.16).

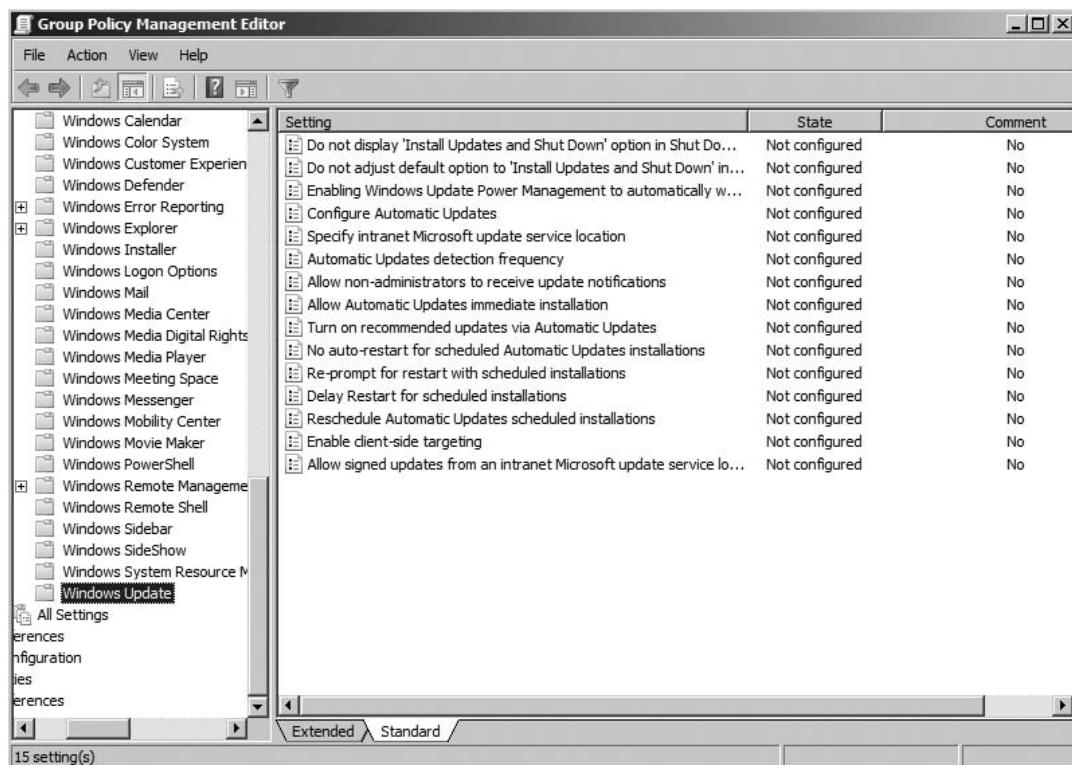
Figure 10.16 Configuring WSUS Clients



6. Locate your newly created policy in the left pane. Right-click the **WSUS Policy** and select **Edit** to open the Group Policy Management Editor.

7. Expand **Computer Configuration | Policies**.
8. Right-click **Administrative Templates** and select **Add/Remove Templates**.
9. Click the **Add** button and select **wuau.adm**. Then, click **Open** to add the template.
10. Click **Close** to add the Administrative Template.
11. Expand **Administrative Templates | Windows Components**.
12. Scroll to the bottom of the list and select **Windows Updates** (see Figure 10.17).

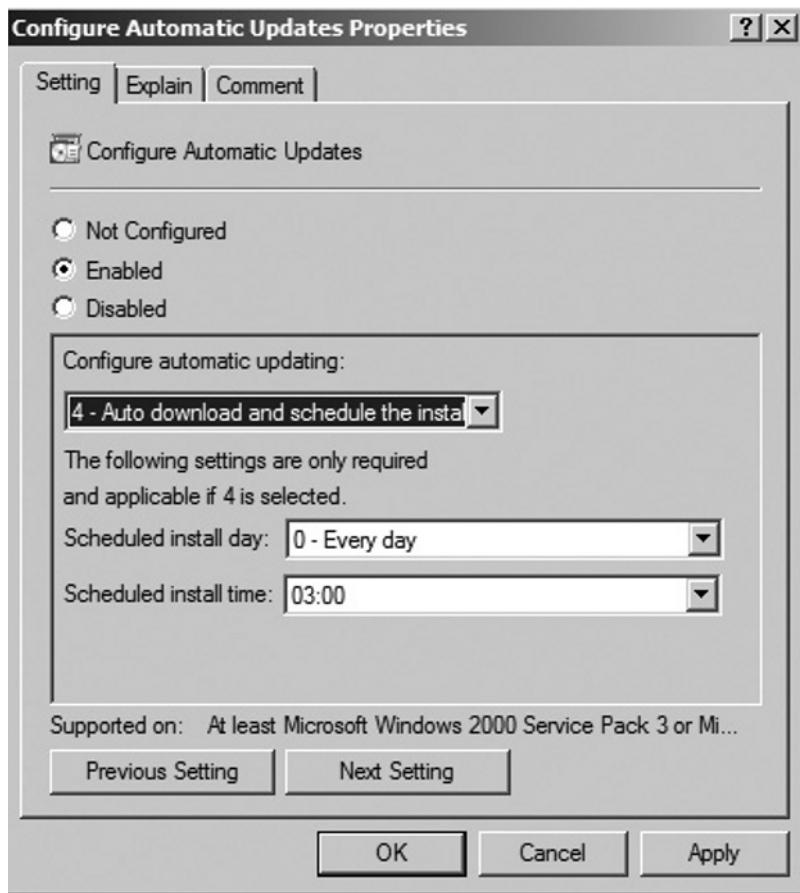
Figure 10.17 The Group Policy Management Editor



13. In the Setting pane, double-click **Configure Automatic Updates** to view this policy's settings
14. Select the radio button for **Enable**, choose Auto download, and schedule the install.

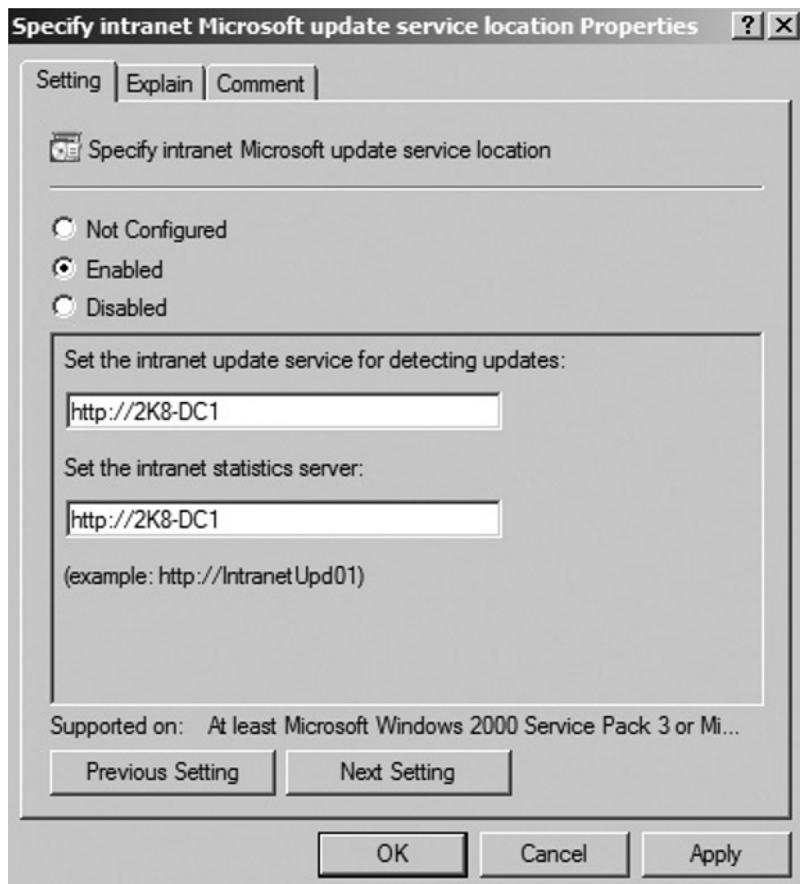
15. Configure a time for the installation that will not be disruptive to the users and then click **OK** (see Figure 10.18).

Figure 10.18 Configuring a Time for the Installation



16. Double-click the policy labeled **Specify intranet Microsoft Update Service location** (see Figure 10.19).
17. Click the **radio button** to enable the policy and specify the URL for the WSUS server that was given at the end of the WSUS setup procedure. If you chose to install this on the default IIS instance on your server, the URL should be your server name.
18. Click **OK**.

Figure 10.19 Enabling the Specify Intranet Microsoft Update Service Location Policy

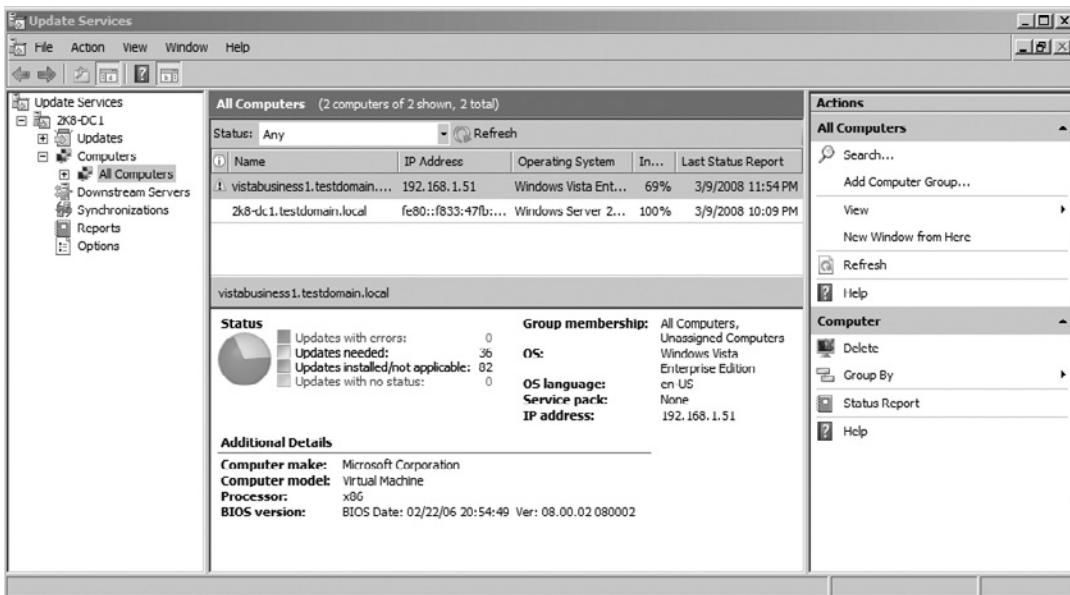


19. Close the Group Policy Management Editor.

Since this policy was applied at the Domain level, all workstations and servers in the domain will receive the policy. These machines will be able to apply the policy if there isn't a GPO filter preventing it from taking effect.

Workstations in the domain will apply this policy the next time they are rebooted or receive policy updates from the server. You can force this by issuing the following command on the workstation: **gpupdate /force**

20. Open the WSUS Administration console to view the clients' statuses once they have registered with the WSUS server. You should be able to view the compliance status and outstanding patches for these machines (see Figure 10.20).

Figure 10.20 Viewing the Clients' Statuses

Application Patching

As you have seen, the Windows Server Update Service can do more than just simple Windows operating system patches. Its reach is much wider, allowing the network administrator to update a number of Microsoft applications. The WSUS engine also provides a rich API that would allow the base functionality of the product to be extended to accommodate special application update scenarios.

In most situations, the elevated risk that is posed by out-of-date software is different from that posed by missing critical updates and operating system patches. It doesn't meet the needs of the organization to look at patch management from only a single perspective. Rather, you might need to configure a number of different computer groups within the WSUS structure to allow for different patch deployment policies. This will allow you to broadly apply Windows patches at the top levels of the hierarchy while maintaining finer control on specific office applications lower down in the tree.

Security Baselines

One of the primary benefits of diligently tackling the challenge of maintaining a common patch level in an environment is to mitigate the risk that security vulnerabilities pose to your corporate operations. These can range from simple Denial-of-Service

attacks through the compromise or loss of corporate data. Given this risk and the potential impact to an organization, it is important the network administrator be aware of the potential threats and the level to which the corporate workstations and servers are able to withstand this kind of exploit.

In a small environment, it is relatively easy to track the deployment of patches as the number of hosts involved is few and the IT team might even be a single person. As the environment grows, though, this challenge becomes impossible to manage manually. Geographical distances between branch offices, the number of machines, and the management burden of tracking the status of each machine quickly become more than even a very focused team can handle.

The security status of the machines becomes important too, as the overall health of the workstations and servers are considered in the holistic picture of the network's health. Maintaining strong passwords, appropriate system logging, and limiting access to internal system components should all be considered in this picture since all of these factors play an important role in determining the appropriateness of enterprise security projects and the evolution of the environment over time.

What Is a Baseline?

The strength of IT systems lies in their ability to change and adapt to changing business dynamics without the need to dramatically rework the business infrastructure. This flexibility comes at a cost as the effort involved in maintaining the environment is shifted from the line-of-business workers to the IT department responsible for effecting these changes. This leads to a more volatile computing infrastructure that is better able to support the business that can enable the business to be more nimble reacting to changing market pressures.

In this kind of dynamic environment, it is important to build your network environment on a firm foundation of best practices that can be adapted to your specific needs. This acts as a standard against which future projects and security configurations can be evaluated for their effectiveness and cumulative risk to the organization. If the network and server infrastructure has been built to tight specifications, it becomes easier to audit the environment against the standard so that IT efforts can be focused on the areas that need special attention. This will also prove invaluable in quantifying the risk associated with specific projects or actions so they can be tailored to your network's specific needs.

Using the GPO Accelerator Tool

Even very experienced network administrators may not have the time and highly specialized skills required to build enterprise-class security infrastructure in a

Windows 2008 domain. Fortunately, Microsoft has released the Windows and Office security guides to provide design guidance and prebuilt templates for security design and deployment. These guides can act as a good starting point for enterprise security but are flexible enough to accommodate almost any forest structure. These can even be deployed in existing environments offering an opportunity to bring your environment into compliance with the security recommendations over time—this needn’t be an all or nothing proposition.

Unfortunately, these recommendations are complicated and require a significant investment of time to plan, test, implement, and deploy. The GPO Accelerator tool is an application package supplied by Microsoft to deploy these settings to the forest, automatically removing the opportunity for operator error and speeding the process up considerably. This tool even offers a capability to deploy a test OU structure that can act as a starting point for a new domain structure, or simply a test bed for future custom implementation.

Any time significant changes are to be made to a live domain, care should be taken to ensure that the environment will be protected and that there are back-out plans that will protect business continuity through the change. To prevent unexpected effects, it is highly recommended that all changes be made in a test environment and labbed extensively before rolling into production. Before using the GPO Accelerator Tool, you should thoroughly read through the Windows Server 2008 Security Guide to plan your security implementation before relying on the tool’s automation for your design. This will allow you to make informed choices as you work through the security policies and will ensure that you are familiar with the tools associated with the deployment of enterprise security, namely: the Group Policy Management Console (GPMC), the Resultant Set of Policy tools (RSoP), the Security Configuration Wizard, and command-line tools.

NOTE

You can download the tools and security guides from the Microsoft Downloads site that the GPO Accelerator Tool enforces.

GPO Accelerator Tool www.microsoft.com/downloads/details.aspx?FamilyID=a46f1dbe-760c-4807-a82f-4f02ae3c97b0

Windows Server 2008 Security Guide <http://go.microsoft.com/fwlink/?linkid=92550>

Office 2007 Security Guide <http://go.microsoft.com/fwlink/?linkid=103573>

Windows Vista Security Guide <http://go.microsoft.com/fwlink/?linkid=74027>

Windows XP Security Guide <http://go.microsoft.com/fwlink/?linkid=14839>

Requirements

The GPO Accelerator Tool can be managed from workstations running Windows Vista SP1 or Windows XP SP3, but requires that the Active Directory Domain Services (AD DS) be running on Windows 2008 Server. Member servers in your environment can be running Windows 2008 or Windows 2003 R2 and all workstation machines in the domain scope of management must be running Windows Vista or XP. It should be noted that Windows 2000 workstations or servers are not supported as either management stations or clients in the domain.

Supported Security Baselines

Within the security recommendations defined in the Windows Server 2008 Security Guide, there are two different configurations that are each appropriate for different network environment configurations. When developing your corporate security specification, it will be important to evaluate the two options to ensure the correct one is chosen to support your needs.

- **Enterprise Client (EC) Environment** In this configuration, Group Policies Objects (GPOs) are used extensively to create a highly differentiated environment to secure different types of server resources and user environments. This is the configuration that is most appropriate for organizations that do not already have a well-defined security baseline or that will be evolving their security requirements over time. The EC configuration will leverage your domain structure with the OUs, GPOs, and sites that are in it to control access and restrict users to appropriate communication channels.
- **Specialized Security / Limited Functionality (SSLF)** In some environments, the need for a very high-security environment dominates the IT landscape—sometimes forcing the business to fundamentally change to support industry or regulatory compliance requirements. SSLF dramatically limits the functionality of the managed resources allowing the network

administrator to make additional services as needed. This can be a significant burden on the IT staff as the level of detail in planning the environment is much greater than is required by the EC Baseline Template and the user experience must be carefully planned so as not to create a deluge of support tickets when common services become unavailable.

NOTE

The SSLF configuration should only be considered appropriate for environments with extensive security requirements and very specialized requirements. For most environments, the EC Baseline Environment is appropriate and provides an excellent starting point for full enterprise security planning.

In Exercise 10.4 we show you how to configure the GPO Accelerator tool.

EXERCISE 10.4

CONFIGURING THE GPO ACCELERATOR TOOL

1. To install the GPO Accelerator tool, download the GPO Accelerator tool from the Microsoft Downloads site.
2. Log on to a domain controller with Domain Administrator privileges.
3. Unzip the GPO Accelerator and run the install program to begin the configuration process.
4. On the welcome screen, click **Next**.
5. Accept the End-user license agreement and click **Next**.
6. Validate the path of the Install and click **Next**.
7. Click **Install** to begin the installation, click **Finish** once the program completes.

Some of the changes that the GPO Accelerator will make to your GPO and Security Policy settings cannot be displayed by the GPMC and Security Configuration Editor. You will need to extend these tools to provide full visibility into these configuration settings. This is an example of the command line available to the GPO Accelerator.

8. Navigate to Start | All Programs | GPO Accelerator | GPO Accelerator Command-line.
9. Type in `cscript GPOAccelerator.wsf /ConfigSCE` and press Enter.
10. You will be prompted with a security warning saying you are changing the SCE tool. Click Yes to continue the process.
11. Click OK to complete the process.
12. To set up the GPO Accelerator as a LAB environment, navigate to Start | All Programs | GPO Accelerator | GPO Accelerator.
13. Double-click the **GPO Accelerator** application in this folder to begin the configuration. Click Next to proceed.
14. On the **Tool Options** screen, select **Domain** to deploy the changes in your domain environment (see Figure 10.21).

Figure 10.21 Configuring the GPO Accelerator Tool



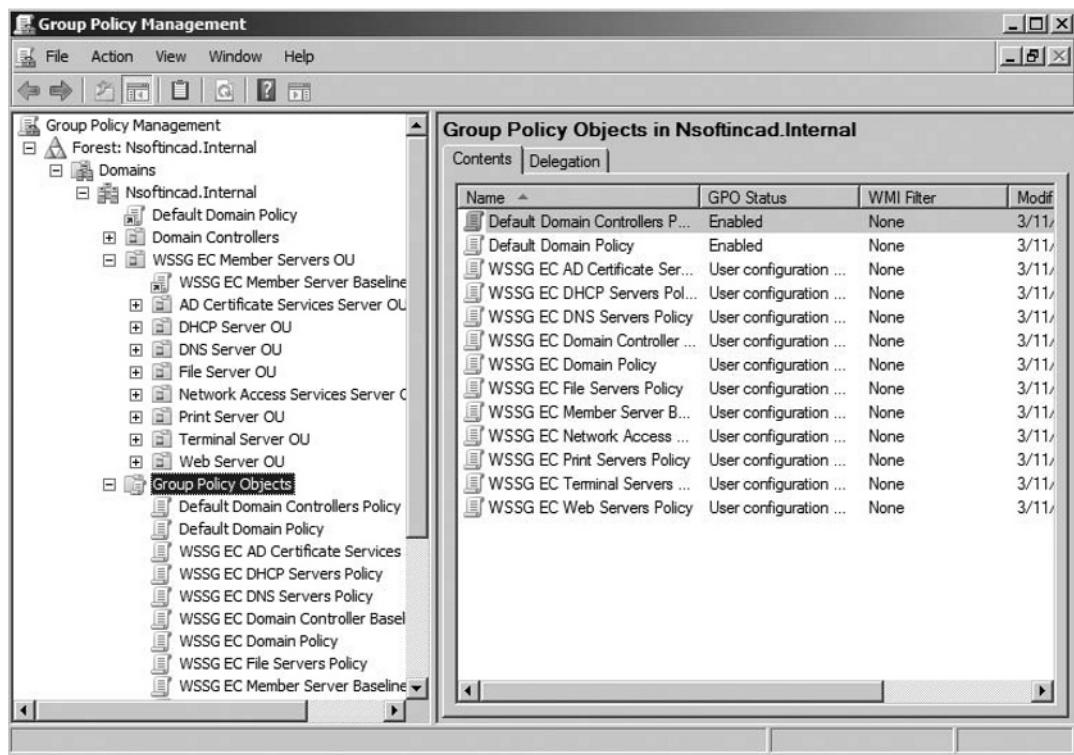
15. On the security Baseline page, select the **Windows Server 2008 Baseline** and click **Next** (see Figure 10.22).

Figure 10.22 Security Baselines

16. On the environment Options screen, **choose the Enterprise Client (EC) environment configuration radio button** and click **Next**.
17. On the Scenario Options screen, **choose the radio button for the lab environment**. This will configure test OUs and GPOs that are already linked (see Figure 10.23). Click **Next**.

Figure 10.23 Scenario Options

18. Review the Configuration options and click **Continue** to complete the installation.
19. When prompted to confirm the change, click **Yes** to continue.
20. Click **Finish** to complete the GPO Accelerator Tool Configuration.
21. To link the domain policy and validate the installation, Navigate to **Start | Administrative Tools | Group Policy Management**.
22. Expand the **Forest** and **Domain** nodes to view the newly created OUs and policies (see Figure 10.24).

Figure 10.24 Viewing OUs and Policies

23. Right-click the domain and select **Link an Existing GPO ...**.
24. Select the **WSSG EC Domain** policy GPO and click **OK**.
25. On the **Main GPMC** screen, select the new policy and promote its Link Order to 1.
26. Right-click the **Domain Controllers OU** and select **Link an Existing GPO....**
27. Select the **WSSG EC Domain Controller** policy GPO and click **OK**.
28. On the **Main GPMC** screen, select the new policy and promote its Link Order to 1.
29. Close the GPMC.

At this point, the GPO Accelerator EC baseline policies have been configured and individual OUs have been configured for a number of different server types. You can test the policies by adding servers in your environment to these OUs to evaluate the policy effects.

The GPO Accelerator Tool is the best way to deploy the security recommendations in the Windows Server 2008 Security guides, allowing the network administrator to configure the environment from a baseline built on Microsoft Best Practices. This tool eliminates much of the work involved in the configuration and eliminates the opportunities for human error inherent in the highly complicated manual setup process.

Using the Baseline Security Analyzer

As systems change, it becomes important to be able to audit the state of the environment to be sure that the security and configuration of all systems involved is aligned with industry best practices and corporate security policy. This means that the network administrator or security officer should be actively engaging with the environment to assess the compliance of host machines with these policies as they are evolved and be able to react to resolve any gaps that should arise.

Some network administrators try to track changes made to the environment to be used as this accounting, but that practice relies on inferred knowledge of the systems and relies on assumptions of the workstations' homogeneity and the 100% effectiveness of patches. In large enterprises, neither of these should be taken for granted and an active audit should be performed to validate system security and overall risk.

These periodic assessments form individual system baselines that can track project effectiveness, security vulnerabilities, and system state over time. This also forms a basis for an evaluative assessment of the network's performance so that positive behaviors can be affirmed and negative effects eliminated. This helps to encourage proper system management especially in networks that have distributed administration or many remote offices where all aspects of security cannot be controlled.

The Microsoft Baseline Security Analyzer (MBSA) fills a different role than either WSUS or the GPO Accelerator Tool. These other tools are used to push updates to workstations or bring machines into compliance with corporate security standards. Unlike these technologies that push policies to the client machines, the MBSA is an auditing tool that can be used to evaluate the actual running state of workstations and servers on the network. This tool contacts each of the machines in the domain to audit the running configurations rather than expecting that the domain GPOs or Security Templates are working.

The output of the MBSA is an analysis of the environment with remediation steps that should be taken to bring the client machines into compliance.

Comparison to Microsoft Update

Microsoft Update acts as a central repository that is authoritative for system patches, critical security updates, feature packs, and other types of system enhancements.

These are important as a reference that can be used to measure the current configuration of a server or workstation against a fully updated ideal. The Microsoft Baseline Security Analyzer uses this database to build this snapshot and then audit machines in the domain for compliance with the ideal.

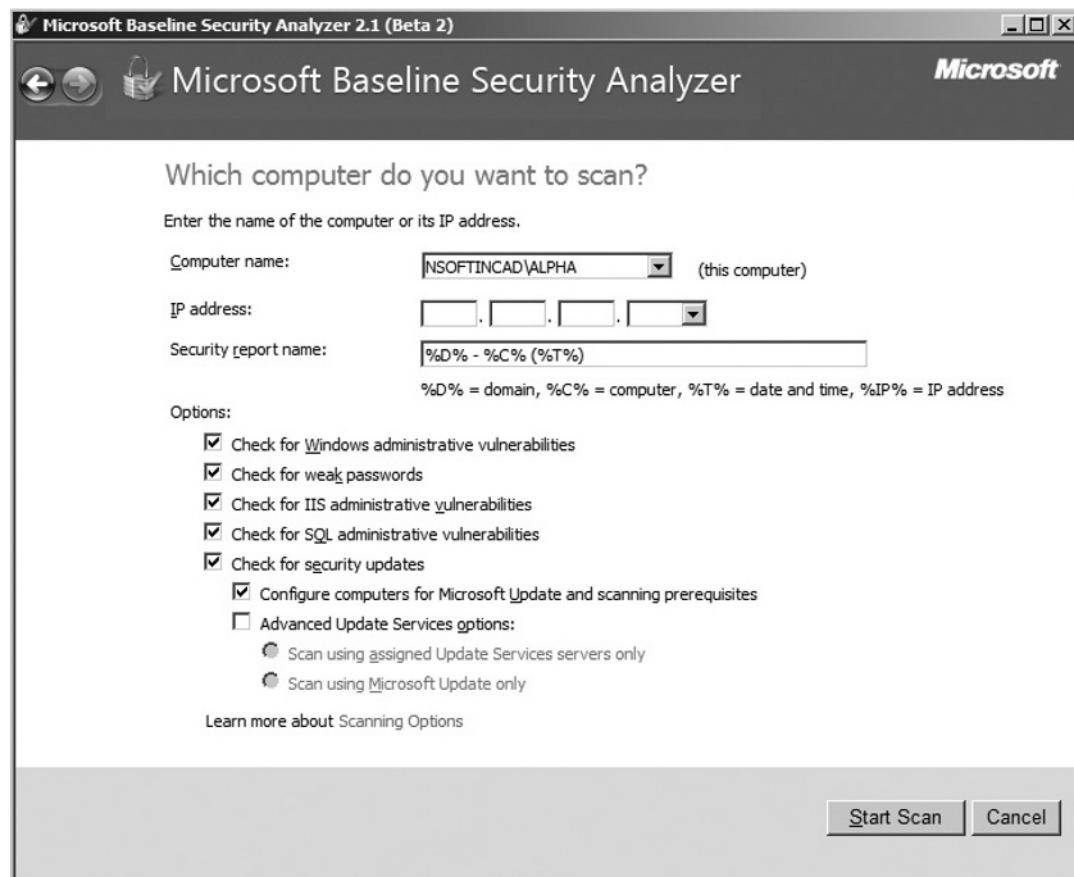
Implementing MBSA

In Exercise 10.5, we will run the MBSA tool against a single machine to audit the configuration of this machine and determine the overall health of this client.

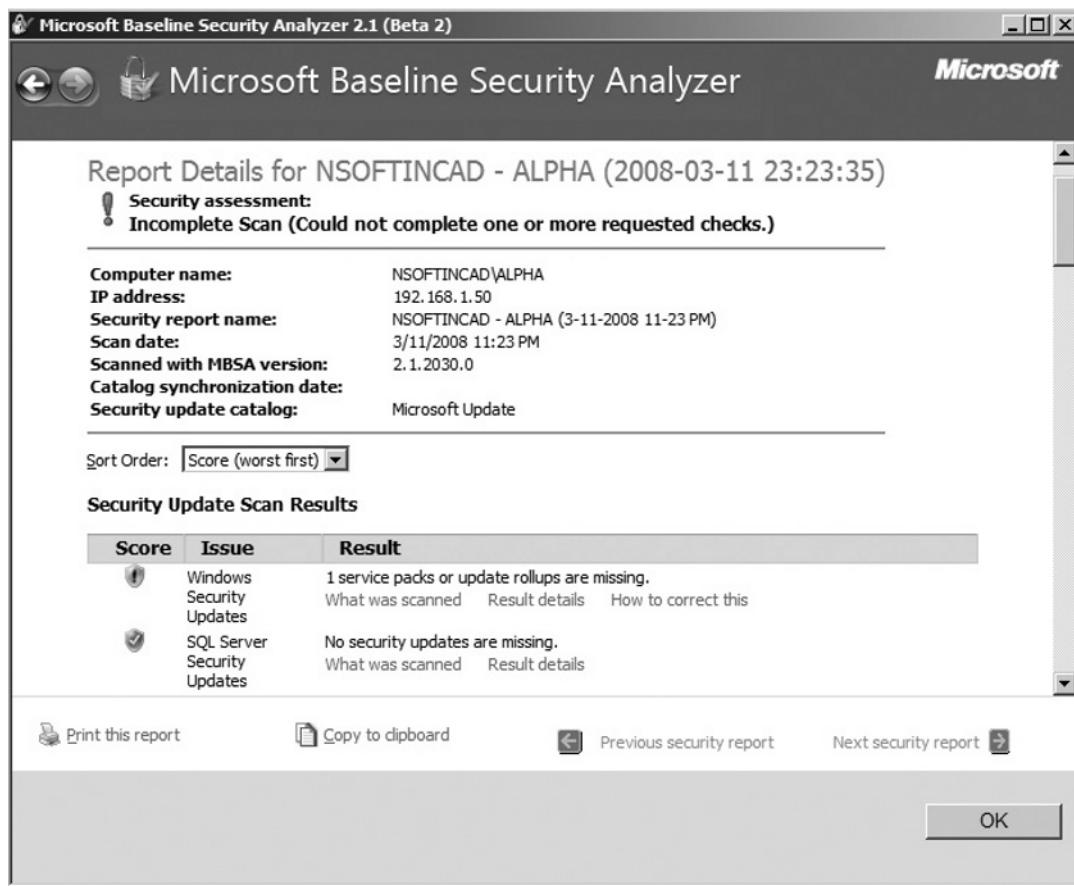
EXERCISE 10.5

CONFIGURING THE MBSA

1. To install the MBSA, log on to a domain controller with Domain Administrator Privileges.
2. Download the **MBSA** from the Microsoft Downloads site.
3. Double-click the **MBSA** executable to start the install process and then click **Next**.
4. Accept the **License Agreement** and click **Next** twice.
5. Click **Install** to confirm the installation.
6. To run the MBSA tool, navigate to **Start | App Programs | Microsoft Baseline Security Analyzer**.
7. On the welcome screen, click **Scan a Computer**.
8. In the computer name, specify the name of the workstation you would like to scan. In this case, select **NSOFTINCAD\ALPHA**.
9. Select the checkbox beside **Configure computers for Microsoft Update and scanning prerequisites** so that any running requirements are resolved in the scanning process (see Figure 10.25). Click **Start Scan**.

Figure 10.25 Configuring the MBSA

10. Review the resulting reports (see Figure 10.26).

Figure 10.26 MBSA Report Details

- Click **OK** to complete the assessment.

From the main screen, you can review the security analysis for this analysis and for any other machines you may have scanned in the past. This provides a historical log of the scanned configurations of your network clients.

Analyzing MBSA Results

The Microsoft Baseline Security Analyzer provides detailed configuration information on all machines that have been passed through the auditing engine. Several different kinds of information are returned in a scan ranging from patch level to application configuration information. Each of these recommendations should be individually considered, but also trends should be evaluated across groups of machines as these

might point to security policy changes that might be done for your domain to improve your risk mitigation strategy.

- **Security Updates** The system update status is compared against the Microsoft Update database to validate that all appropriate patches have been installed on the server or workstation. Any missing software or needed updates are enumerated so the system administrator can take immediate action to resolve the deficit.
- **Administrative Vulnerabilities** These checks ensure that the administrator and guest accounts have been properly secured and that all remaining accounts on the computer or domain (if run on a domain controller) have secure passwords following the domain policy. This also checks to be sure that the system has a defined way to get updates and that the Internet connection is appropriately firewalled.
- **System Information** This check is a general validation of the system configuration to ensure that system events are being appropriately audited and that ingress points such as shares and services are protected.
- **IIS Scanning** As many system compromises are exposed through Internet Information Server (IIS) and misconfigured security rights, this application is given special attention by the MBSA tool. Service accounts are validated and the lockdown settings are checked to ensure that the surface area of attack is kept as small as possible while still maintaining server function.
- **SQL Server Results** Even when SQL server is not installed as a stand-alone product, many applications and utilities use SQL as the backend datastore. Issues surfaced here are primarily related to the SQL authentication and log on accounts ensuring that the passwords and system accounts are secured from compromise.
- **Desktop Application Results** These results bring to light vulnerabilities and update issues tied to Internet Explorer and Microsoft Office. These primarily are relation to access rights and protected access to the Internet through the programs.

In each one of these cases, detailed information on each error and the actual data collected is presented in the overall report. Also, resolution steps have been compiled for many of the common issues you are likely to face. This overall guidance can significantly lower the administrative effort required to manage the risk of compromise on these systems.

NOTE

When you are using the MBSA in the real world, the tool is often overlooked until there is an active problem affecting the systems on your network. While it can be a powerful troubleshooting tool that can often help you determine the root cause of an outage or system problem, the best use of the tool is as a proactive assessment of your environment.

In practice, it is not practical to analyze a large corporate environment constantly. It does, however, make sense to include the MBSA audit in a periodic snapshot of your domain. Most organizations find it useful to do an entire snapshot on a monthly or quarterly basis. Even this generates a lot of data, but it does provide a good historical record should problems arise and allows periodic spot-checking of the system health on a workstation. These should be reviewed, though, on domain controllers and servers that are hosting mission-critical services or that are in direct contact with the Internet for inbound connections.

The MBSA should also be considered an important precursor to large IT projects that have the potential to have broad scope or high-risk operations. For example, when performing a domain rename or a domain union with the Active Directory Migration Tool (ADMT), it can be helpful to have the MBSA reports on the servers and workstations being moved since individual configuration issues can have a dramatic impact on security translation.

System Health Models

Managing the health of workstations and servers in your environment is more than just ensuring that the operating system is up-to-date and that a reasonable baseline of security policies has been applied. Applications on individual machines do not work in isolation and will often times rely on one another to provide data and computing resources to the end user. These interactions of systems and services must be maintained in concert; otherwise, single applications could be well maintained, but still not supply the overall solution they should.

What Is a System Health Model?

Looking at a single application in an environment will only provide a one-dimensional view of system functions and the health of the environment. An organization that relies on Microsoft Exchange to provide e-mail services would certainly want to monitor and validate the function of Exchange itself in evaluating

the health of the environment. This does not necessarily give the network administrator enough information to understand what is happening on the network since a number of different systems contribute to the overall function of the system.

In this case, it is important to look at the business function of providing enterprise e-mail rather than just looking at the Exchange server itself. Other resources such as the Active Directory and DNS will play critical roles in the delivery of the business function and must be considered when looking at the delivery of the service.

To manage these systems as an overall service level, higher-level management tools are required. Microsoft System Center Operations Manager 2007 (SCOM) and System Center Essentials are able to aggregate a number of different system performance metrics and availability statistics into account to present a true picture of the health of an individual system. Windows Server 2008 provides additional metrics automatically that allow these systems to monitor the AD DS role, DNS, and other core server role-based measurements.

Developing a Health Model

When you are developing a health model, it is important to have a thorough understanding of your network systems (workstations and servers) and how they map back to service functions you are providing. For each of these, a service level should be defined to outline availability, response, and maintenance expectations for each of these systems. Finally, these can be mapped into your systems management software to provide reporting on a functional level.

These health metrics can also be built into a network access control NAP Health Service Validator within NPAS to ensure that workstations are meeting certain health requirements to participate in network communications. This will tie resources like WSUS and Microsoft Update requirements into network control to ensure that workstations and servers are being maintained correctly if they are to talk to other domain resources. This allows for strong enforcement of health requirements tied to your update and management policies.

Summary of Exam Objectives

Patch and Compliance Management are vital disciplines to the risk management of an organization that help ensure security standards are enforced, that make sure known risks for external penetration are mitigated, and which provide a broad understanding of the state of your network environment at any given time. The Compliance management cycle is comprised of three different dynamics that all must be executed and kept in balance to provide the optimal balance between administrative effort and risk mitigation. This balance is found between the disciplines of system auditing, policy enforcement, and enabling machines to receive updates. To achieve this goal, Microsoft provides a number of tools to manage all aspects of the process cycle.

Exam Objectives Fast Track

Patch Management

- Make sure you thoroughly understand the business and the landscape of the technology environment before you settle on a policy for your environment. It is important to let the needs of the business lead rather than simply implement technology without a focus.
- You should implement enabling technologies such as the Windows Server Update Service to allow the workstations and servers in your environment to get updates and to bring themselves into compliance with the corporate standard.
- Enforcement technologies such as the policies and standards implemented by the GPO Accelerator tool in accordance with the Microsoft best practices Security Guides allow the network administrator to make decisions about the security requirements on the network and enforce them through group policies.
- Enforcing and enabling technologies work on a push basis, sending control information to the workstations in your network with any real authoritative feedback as to the compliance of these network machines with the standards. Auditing technologies such as the Microsoft Baseline Security Analyzer allow you to get a picture of the environment as a whole. From this vision, you can address specific security problems and spot trends across multiple machines. This will act as a starting point for network troubleshooting since you will have historical data about the status of your domain machines.

Windows Server Update Services

- The WSUS utility allows network administrators to centrally control the patch management of the core operating systems, as well as major Microsoft applications deployed across the enterprise.
- WSUS is highly flexible and can be deployed in a hierarchical fashion with central WSUS servers passing update services and metadata to subordinate servers to control branch offices or other sites with limited network access.
- WSUS provides a single aggregation point for all operating system and Microsoft application updates keeping the network traffic within the core network and allowing the network administrator to only deploy patches and updates that have been approved for distribution.
- Network administrators should implement a test environment on the network to test patches before they are deployed to the entire network. This includes testing to be sure there are no conflicts with different images and hardware configurations, as well as full testing against mission-critical applications on the network.
- WSUS can update all of the currently supported Microsoft operating systems by comparing the running configurations of each of these against the patch database maintained as part of the Microsoft Update service on the Web. Once this comparison is done, the client workstation or server can download the appropriate patches from the WSUS server using the BITS service and then will apply the patches as they become available.
- Once WSUS has been deployed onto a network, it is important to create Group Policy Objects to allow the workstations and servers to find the WSUS servers. Otherwise, these machines will continue to contact the Microsoft Update site directly and will be outside the scope of management for the server.

Using the GPO Accelerator Tool

- The GPO Accelerator Tool is an automated tool to deploy Group Policy Objects that allow a network administrator to bring domain servers and workstations into compliance with the Microsoft Best Practices Security Guides.
- This tool can be run to provide two different security templates:

- Enterprise client (EC) Environment** This is a general security policy that is most appropriate for an enterprise computing environment. This policy set acts as a good balance between security and usability, ensuring end-users are able to contact services they expect to see in the network while ensuring these communications are conducted in a safe manner.
- Specialized Security/ Limited Functionality (SSLF)** This configuration is highly restrictive and should only be employed in very specialized environments after significant testing. These GPOs lead with high security as the primary focus, trading usability and services for the network protection.
- This tool can be run in two different modes. The LAB mode will create organizational units for testing that can differentiate various server roles and user types with GPOs bound to each of them. This can be a good foundation for a new network that does not already have a complicated OU structure. This tool can also be run in production mode where only the GPOs are created so the network administrator can manually link them into his network as needed.
- Once the GPO Accelerator Tool has been run, it is important to remember to link the domain policy and the domain controller policy to their respective containers and to set their application precedence to the top level to ensure they are processed before any other GPOs bound there.

System Health Models

- Microsoft System Center Operations Manager 2007 (SCOM) and System Center Essentials are able to aggregate a number of different system performance metrics and availability statistics into account to present a true picture of the health of an individual system.
- Windows Server 2008 provides additional metrics automatically that allow these systems to monitor the AD DS role, DNS, and other core server role-based measurements.
- When you are developing a health model, it is important to have a thorough understanding of your network systems (workstations and servers) and how they map back to service functions you are providing.

Using the Microsoft Baseline Security Analyzer

- The MBSA is an auditing tool that is able to poll machines in the domain to validate their compliance with the domain-approved patch levels as well as cursory security constraints.
- This generates reports in XML format for each computer scanned that can be used as a historical record of the health of the client computers acting as an invaluable troubleshooting tool. It is often helpful to perform periodic scans of the domain at regular intervals as a way to manage compliance. A balance should be struck, however, between the need for current data and the impact on the machines due to the audit.
- The MBSA tool must be able to enumerate the machines in the domain from DNS and contact the Administrator shares on each of the machines with local administrator credentials. The easiest way to do this is to always run the scan from an account that is part of the domain administrator group, though other delegations could be made.

Exam Objectives

Frequently Asked Questions

Q: There are many different products out there for patch management and compliance control. How can I be sure I'm choosing the correct products and deployment?

A: The point of rolling out patches and considering a corporate compliance strategy comes down to risk management and tolerance that your organization has for risk. In some environments, the risk might be relatively small because there are only a few machines or the machines could be primarily deployed in very controlled lab settings. In other networks, downtime might be expressed as immediately realized lost revenues and other application requirements might prevent strong security practices.

Because of these types of differences, it is important to consider your tolerance for risk and the business requirements driving patch and compliance management before looking at individual technologies. Once you have this business picture of your environment, you will be able to choose the products and technologies that will meet your needs. You have to make sure you are not leading the solution with the technology—technology for its own sake never lasts and is hard to justify.

Q: I have implemented WSUS, but many of my workstations are not appearing in the Computers tab in the WSUS management console. How can I be sure these workstations and servers are getting updates?

A: The best way to manage the assignment of computers into WSUS is through the application of Group Policy Objects. Usually machines that are not getting their updates from WSUS are having GPO problems where another policy is superseding the WSUS policy, a local policy is overriding, or they are not in the scope of management for the policy due to Our GPO filtering. The best way to troubleshoot this would be to use the Resultant Set of Policy tools so you can see if this policy should be applied to the trouble machines.

Once you are sure the policy should be applied, it is often helpful to look at your DNS to be sure the workstations are finding domain resources correctly. You can also force a GPO to take immediate effect using the **gpupdate /force** command.

Q: I have a number of applications that are not Microsoft products for which I need to manage patches, but I don't know if WSUS can manage updates for these applications?

A: WSUS is a highly targeted tool for managing updates in the Microsoft space and has great flexibility. Unfortunately, it does not work with all products. In these situations, you will generally look at managing patches through GPO-mediated application deployments or through Microsoft System Center Configuration Manager or System Center Essentials.

Q: What if I have deployed a patch through WSUS to my environment and it is causing a problem? Is there anything I can do?

A: Many patches can be uninstalled or rolled back through the WSUS console, though some will not have this option because the update doesn't support reversion. For this reason, it is important you have implemented a good testing plan to reduce the risk of a patch causing problems in your production environment. Usually if there is a known problem with a patch, an update will be released quickly. In cases where an uninstall is not an option, this may resolve the problem.

Q: I am trying to use the Microsoft Baseline Security Analyzer to archive baselines of all of my domain machines on a regular basis. I am getting errors from many of my computers telling me the computers I am trying to scan are not available or cannot provide configuration information. What can I do to be sure a domain scan of these computers hits all of my machines?

A: The MBSA tool uses DNS to enumerate all of the servers and workstations in the domain so they can be contacted. These computers should be appropriately registered in both forward and reverse DNS. If duplicate entries or scavenging problems exist, some of your machines may be missed.

MBSA must also be able to connect to each computer on the Admin\$ share. This means each of these computers must allow the scanning computer to make the connection through the firewall and that the account being used to perform the scan should have local administrator privileges. You can ensure this by using an account that is a member of the domain administrators to perform the scan.

Q: I am having security problems in my domain and would like to use the GPO Accelerator Tool to implement security policies across my domain. How do I ensure that specific security concerns that I have are addressed when I deploy the settings in the tool.

A: The GPO Administrator Tool deploys the security changes enumerated in the Windows Server 2008 Security Guide for the domain. There are also associated security guides for the additional workstation operating systems that are deployed to the workstations as part of the computer OU policies. It is important to review these security guides to be familiar with the details of the security changes to be made. These changes are an implementation of a best-practices baseline, but these should not be considered the single security implementation for your domain. You will, most likely, have specific business-driven security requirements that may not be included in the provided templates. The structure built by the GPO Accelerator Tool is a starting point from which the network administrator should build his own policies.

Self Test

1. You are the network administrator for a small company with ten Windows 2008 servers and 50 workstations in your domain. Currently, all of these machines are not being managed by any update policy and each may have individual settings that allow them to access the Internet to get updates. You would like to form a plan that will enable the workstations to receive updates with a minimum impact to the bandwidth footprint. What steps would you take to enable these machines?
 - A. Configure a local policy on each machine to force them to contact the Windows Update site every evening at midnight and apply all updates.
 - B. Create a Group Policy Object that would specify an update server and apply all approved policies.
 - C. Implement the Windows Server Update Services in your network and begin to approve updates on a regular basis.
 - D. Run the MBSA to determine what updates are missing on every machine.
 - E. Since this is a small environment, assign a network administrator the task of touching each machine once a week to ensure that patches are being applied.
2. As the network administrator of a large corporate enterprise, it is your responsibility to ensure that all of the machines on your network are running the most current set of approved patches and updates. It is also important you are aware of any operating system security holes that have been introduced by some of your traveling power users who take their laptops with them as they go to client sites. What steps should you take to validate that workstations are in line with company policy?
 - A. Run the Microsoft Baseline Security Analyzer against the domain on a regular basis to poll the workstations.
 - B. Implement WSUS to push patches to the workstations.
 - C. Configure the lockdown settings outlined in the Windows Server 2008 Security Guide.
 - D. Require that every machine be attached to the domain to log on.
 - E. Turn on security auditing on the local machines.

3. The company for which you are working started out as a very small organization where you were the only IT person, but the business is growing rapidly. You would like to protect access in your environment and enforce compliance with a single security standard for all server access. Because of the rapid growth, you want to implement changes that are centrally managed, but you are still small enough to make structural changes without undue hardship to the business. What technologies should be at the core of your security compliance strategy?
- A. Implement the Windows Server Update Services.
 - B. Create a domain security policy that enforces password complexity requirements.
 - C. Implement the base OU and GPO structure provided in the GPO Accelerator Tool.
 - D. Run the MBSA to determine what updates are missing on every machine.
4. You are working as the network administrator for a large enterprise with several large offices across the globe. Microsoft has released a major service pack for Windows Vista that is deployed to your workstation operating system at all locations. You should take several steps to validate that the patch is safe before rolling it out to all locations. What should be your first step in an appropriate rollout stratagem?
- A. Deploy the service pack in a lab environment to ensure all mission-critical and line-of-business applications work as expected.
 - B. Deploy the service pack across the organization on a rolling schedule.
 - C. Deploy the service pack to a single site.
 - D. Deploy the service pack to cross-functional test groups in each department of your organization.
 - E. Deploy the service pack to test machines in a lab environment to test the OS.
5. The network that you administer has a number of different applications running. Your boss would like you to implement a patch management solution that will cover the majority of the Microsoft operating systems and programs in your environment. Which major applications will WSUS be able to update?
- A. Configure a local policy on each machine to force them to contact the Windows Update site every evening at midnight and apply all updates.
 - B. Create a Group Policy Object that would specify an update server and apply all approved policies.

- C. Implement the Windows Server Update Services in your network and begin to approve updates on a regular basis.
 - D. Run the MBSA to determine what updates are missing on every machine.
 - E. Since this is a small environment, assign a network administrator the task of touching each machine once a week to ensure patches are being applied.
6. The director of IT would like you to deploy a patch management solution that will be capable of ensuring all workstations and servers in your network are able to get operating system patches that have been internally tested. You are planning to deploy WSUS to meet this need. Unfortunately, you have a number of legacy machines in your environment. You will need to upgrade a number of workstations before they will be able to participate in WSUS updates. Which machines will you have to replace or upgrade?
- A. Windows Server 2000 SP2
 - B. Windows ME
 - C. Windows XP SP2
 - D. Windows 2000 Workstation SP4
 - E. Windows NT Server
7. Your network has been built using a highly decentralized model with a central headquarters and large independent branch offices, each with their own IT departments and standards. You would like to implement WSUS in your environment but need to ensure that each branch office has control over the patches deployed in their branch offices. How should you configure WSUS to ensure these requirements are met?
- A. Implement WSUS as an enterprise service and allow the branch offices to manage their own group policies to control whether or not the machines on their local segments will attach to the central WSUS servers.
 - B. Implement a centrally configured WSUS server and additional WSUS servers at each branch office that will receive their patches from the central site, but be able to control the patch approval and deployment at each site.
 - C. Configure WSUS at the central site but still allow the individual branch offices to go directly to the Microsoft Update site to get their patches.
 - D. Implement WSUS independently at each of the branch offices with separate site GPOs controlling WSUS membership.

8. You are the network administrator of a large enterprise planning to deploy WSUS servers as a centralized patch management platform. You would like to ensure this service is implemented in a highly available manner. You want to be sure you are providing an adequate database structure to support this environment. What database configuration should you choose to provide the appropriate availability for your implementation?
 - A. Allow the WSUS servers to use their internal database to manage the datastore.
 - B. Implement a cluster of SQL 2005 databases to house the datastore.
 - C. Store the database on a server running SQL 2005.
 - D. Configure Microsoft Access 2007 to house the datastore.
 - E. Use the SQL 2000 Cluster you already have in your environment to house the databases.
9. You are planning a testing lab environment so you can evaluate the impact of patches on your business before releasing them for wide deployment. You would like to keep the environment as small as possible so your costs are controlled, but you also need to ensure that patch deployment will not cripple your business. What resources should you implement in your patch testing lab?
 - A. You must represent every application you have deployed in the wild in your lab environment.
 - B. You should duplicate all servers in your server environment to be sure there will be no conflicts.
 - C. You should have a representative of each major workstation base image in your test environment.
 - D. You should have an environment capable of running each of the mission-critical applications on your network.

10. You are planning to delegate the management of WSUS patches to lower level systems administrators on your network. You are concerned that the deployment of some kinds of patches might pose a larger risk to your environment without thorough testing and high-level approval. To address this, you are planning a two-level WSUS deployment where your systems administrators will only be able to deploy certain types of patches, but you will still be able to receive the full patch set centrally. Which classifications should you exclude from the lower level deployment?
- A. Drivers
 - B. Service Packs
 - C. Critical Updates
 - D. Definition Updates
 - E. Update Rollups

Self Test Quick Answer Key

- | | |
|----------------|-------------------|
| 1. B, C | 6. A, B, E |
| 2. A | 7. D |
| 3. C | 8. B |
| 4. E | 9. C, D |
| 5. B, C | 10. A, B |

Appendix

MCITP Exam 647

Self Test Appendix

Chapter 1: Name Resolution and IP Addressing

1. Steve is an IT administrator who recently joined an electronics manufacturing company. His company has decided to use computer names of 16 characters. One day, a user complains that she is not able to reach a Windows 2008 server named memberserver120A. While troubleshooting, Steve notices there are two names for the Windows 2008 Server in computer properties, a 16-character name, memberserver120A, and a 15-character name, memberserver120. What is this 15-character computer name?
 - A. This is a native computer name.
 - B. This is a NetBIOS name.
 - C. This is fully qualified domain name.
 - D. This is a secondary host name.

Correct Answer & Explanation: **B.** Even though host names can be long, NetBIOS names are limited to 15 characters. In this case, host names assigned are longer than 15 characters, while the NetBIOS names are truncated to 15 characters. All Windows operating systems have two names, a DNS host name and a NetBIOS name.

Incorrect Answers & Explanations: **A, C, and D.** Answer A is incorrect because there is no such thing as a native computer name. Answer C is incorrect because *memberserver120A* or *memberserver120* do not have domain names in front of them and are not Fully Qualified domain names. Answer D is incorrect because there are no such things as secondary names

2. What is the root domain name of a namespace in FQDN alpha.nsoftad.internal.?
 - A. alpha
 - B. nsoftad
 - C. internal
 - D. There is no root domain in FQDN.

Correct Answer & Explanation: **C.** Answer C is correct because root domain is the right-most name in the FQDN.

Incorrect Answers & Explanations: **A, B, and D.** Answer A is incorrect because alpha is a host name. Answer B is incorrect because nsoftad is a domain name to which the computer belongs. Answer D is an incorrect statement.

3. You are the network administrator for your company and have upgraded all your computers to Microsoft Windows Server 2008. Client computers are running Microsoft Windows Vista. The DNS service has been installed on a member server within the company domain. You want to provide fault tolerance for your zone so that name resolution can still continue if the DNS server goes offline. You plan to add another DNS server to the domain, but need to configure the new DNS server role in the appropriate role. What should you do?
- A. Configure the new server as a secondary DNS server.
 - B. Configure the new server as a master name server.
 - C. Configure the new server as a caching-only server.
 - D. Configure the new server as a DNS forwarder.

Correct Answer & Explanation: **A.** Answer A is correct because the first DNS server service is installed on a member server and holds a primary copy of the zone. Any further addition of DNS servers for the zone will be as secondary servers. Secondary servers have a read-only copy of the zone database.

Incorrect Answers & Explanations: **B, C, and D.** Answer B is incorrect because master name servers are basically the primary servers and are the source of the zone file for secondary servers. Answer C is incorrect because caching-only servers do not hold any zone information. Answer D is incorrect because A DNS forwarder is not a specific DNS role. When configured as a forwarder, a DNS server can forward requests it cannot resolve to another specific DNS server.

4. Connor is an IT manager of a food supply company. He has upgraded his company's domain controllers to Windows Server 2008. The company is planning to open a new remote branch that will be connected to the corporate office via a 128-kbps WAN link. Connor wants to install a DNS Server service in the branch office to limit the DNS query traffic going over the slow WAN link and to improve performance; however, he does not want to configure any zones on that DNS server or install a domain controller. What shall he do?
- A. Install a secondary DNS server in the branch office.
 - B. Configure a DHCP server to provide the zone configuration.
 - C. Install a caching-only DNS server in the branch office.
 - D. Connor cannot install a DNS server without zones.

Correct Answer & Explanation: **C.** Answer A is correct. Caching-only DNS servers do not require any zone configuration. They just keep the cache information of all the queries resolved.

Incorrect Answers & Explanations: **A, B, and D.** Answer A is incorrect because setting up a secondary DNS server requires secondary zone configuration.

Answer B is incorrect because DHCP does not host any zone. Answer D is an incorrect statement.

5. What steps does a DNS client take before it sends out the query to a DNS server for resolution?

- A. A local resolver cache is checked.
- B. The HOSTS file is checked.
- C. It broadcasts to a local subnet.
- D. It contacts the WINS server.

Correct Answer & Explanation: **A and B.** Answers A and B are correct because when a client requests name resolution information, the DNS service first checks the local resolver cache and then the HOSTS file before sending out the request to a DNS server.

Incorrect Answers & Explanations: **C and D.** Answer C is incorrect because the DNS client does not broadcast before querying the DNS server. Answer D is incorrect because WINS is not used to resolve DNS queries.

6. Steve is a Windows administrator of a small printing company. The company has a Windows 2008 domain Qprint.net and his company recently purchased Microsoft Exchange Server 2007. He has installed the Exchange server, mailsrv, but he can't receive any e-mails. What must Steve do to ensure that e-mails are received to his Exchange Server?

- A. Update the PTR record on the ISP DNS for Exchange.
- B. Create the MX record on the ISP DNS for Exchange.
- C. Update a record on the ISP DNS for Exchange.
- D. Create an SRV record for Exchange Server.

Correct Answer & Explanation: **B.** Answer B MX record, is a mail exchange record and must be created on a public DNS server of ISP. Without that ISP, DNS would have no idea where to resolve requests for the mail server.

Incorrect Answers & Explanations: **A, C, and D.** Answer A, C, and D are incorrect because PTR is a pointer record, A is a host record, and SRV is a service record and not used for mail servers.

7. Your company has decided to upgrade your Windows 2003 network to Windows Server 2008. You start with the servers and complete the migration of the Windows 2003 servers and services to Windows Server 2008 without trouble. The DHCP and WINS servers provide their services properly with few issues. You leave the WINS configurations and DHCP scopes as they were before. Your Windows 2008 DHCP server was configured to deliver the default gateway, but the DNS servers were manually configured on clients. You have your support technicians begin the process of upgrading the Windows XP workstations to Windows Vista. During the process, they notice there is an option to obtain DNS automatically, and they select that option in order to match the Obtain An IP Address Automatically option. When they attempt to browse the Internet, they can't locate any resources. What is the most likely cause of the problem?
 - A. The technicians need to restart the machine for the changes to take effect.
 - B. The DHCP server does not have the DNS information.
 - C. The DHCP configuration from the Windows 2003 server that was migrated will not properly serve the Windows Vista workstations.
 - D. You need to manually remove the old DNS entries from the Advanced menu tab.

Correct Answer & Explanation: **B.** Answer B is correct because the previous DHCP configuration did not have the DNS information in it since the DNS addresses were manually entered in the DNS client. Once the technicians choose the Obtain DNS Server Address Automatically option, the previous manual information is lost.

Incorrect Answers & Explanations: **A, C, and D.** Answer A is incorrect because there is no reboot required after changing DNS information on clients. Answer C is incorrect because it is not a true statement. Answer D is a false statement as well.

8. Shannon's company has a Windows Server 2008 domain. All of her company's servers run Windows Server 2008 and all of the workstations run Windows Vista. The company's DHCP server is configured with the default settings and

all of the Windows Vista machines are configured as DHCP clients with the default DHCP client settings. Shannon wants to use DNS dynamic updates to automatically register the host record and the PTR record for all of the company's workstations. What must she do to accomplish her goal?

- A. Nothing. The default settings are sufficient.
- B. Configure the DHCP server to always Dynamically update DNS and PTR records.
- C. Configure the DHCP server to Dynamically update DNS and PTR records only if requested by the DHCP clients.
- D. Configure the workstation to use dynamic updates.

Correct Answer & Explanation: **A.** Answer A is correct because the default settings of the Windows Vista and Windows 2008 DHCP server are enough to accomplish the task.

Incorrect Answers & Explanations: **B, C, and D.** Answer B is incorrect because this is enabled in default settings. Answer C is incorrect because it is not a valid option. Answer D is incorrect because Windows Vista machines are configured to dynamically update DNS by default.

9. Jasper is a systems administrator of a marketing company. The company has a domain called nsoftad.com and support.nsoftad.com. All servers are running Windows 2008. Jasper has a delegated support.nsoftad.com to another DNS server; however, he wants to ensure that whenever a new authoritative name server is added for support.nsoftad.com zone, the DNS server for nsoftad.com is notified. What should he do?

- A. Configure a stub zone on the DNS server within the parent domain.
- B. Using the Name Servers tab from the support.nsoftad.com zone, configure the DNS server to notify the DNS server in the parent domain of any changes.
- C. Configure a DNS server within the nsoftad.com zone to be a secondary server to the support.nsoftad.com zone.
- D. Configure all zones to store information within Active Directory.

Correct Answer & Explanation: **A.** Answer A is correct. By configuring a stub zone for support.nsoftad.com on the authoritative DNS server of nsoftad.com, any updates made to the name server records for support.nsoftad.com zone would be updated on the parent zone nsoftad.com.

Incorrect Answers & Explanations: **B**, **C**, and **D**. All these answers do not address the situation at hand effectively.

10. Steve is a network administrator of a large company. All of the company's ten domain controllers and 50 member servers are running Windows Server 2003. The company is planning to retire WINS servers and has moved to DNS for name resolution; however, there are a few legacy applications requiring WINS-like name resolution without using FQDN. Steve has heard about the new feature of globalnames zone in Windows Server 2008 to address this issue. He upgraded one of his domain controllers to Windows Server 2008. However, when he tries to configure the globalnames zone, he is unable to do so. What could be the reason for this? (Choose all that apply.)
- A. All the domain controllers need to be running Windows Server 2008.
 - B. The forest level is not set to Windows Server 2008.
 - C. All the member servers need to be running Windows Server 2008.
 - D. There is no such feature as the globalnames zone.

Correct Answer & Explanation: **A** and **B**. Answer A and B are correct. For the globalnames zone, the forest level has to be at Windows Server 2008, which requires all domain controllers to be running Windows Server 2008.

Incorrect Answers & Explanations: **C** and **D**. Answer C is incorrect because member servers are not required to be on Windows Server 2008 to utilize the feature. Answer D is a false statement.

Chapter 2: Designing a Network Access Strategy

1. You are implementing a Windows 2008 network that will rely on NAP to ensure that clients participating on the network always have updated antivirus definitions before they are able to participate on the network. When these clients log on, they will be required to request access to the network and assert their fitness to access domain resources. This process is an example of?
 - A. Authentication
 - B. Authorization
 - C. Access
 - D. Accounting

Correct Answer and Explanation: **B.** Authorization is the process of validating that an authenticated security principal has the rights to perform an action on a system.

Incorrect Answers and Explanations: **A, C, and D.** None of these choices would grant the clients privileges to log on. Authentication is the process of validating that an asserted credential is valid. Access is an example of an activity that an authenticated user would seek authorization for. Finally, accounting is the logging of the outcomes of the authentication and authorization processes.

2. You are planning to implement a network access security plan that will use the Windows System Health Agent (WSHA) to issue workstations' SoH declarations to the NAP Server. You are concerned that some workstations will not be able to participate on the network after NAP has been enabled. Which operating systems will you have to upgrade?

- A. Windows XP SP2
- B. Windows Vista SP1
- C. Windows Server 2008
- D. Windows Server 2003 R2

Correct Answer and Explanation: **A and D.** The minimum requirements to be able to run NAP are Windows Server 2008, Vista SP1, Windows XP SP3.

Incorrect Answers and Explanations: **B and C.** Both of these operating systems are already compatible with NAP and the health agents. No additional upgrades are required for these hosts to fully participate on the network.

3. You are planning to implement NAP on your network with a variety of Enforcement Clients (NAP EC) that will tie it to appropriate enforcement points. You are planning to use the 802.1x protocol as the authorization component of NAP to validate computer certificates for domain authentication. Which network access technologies can this solution control?
- A. Terminal Services Connections
 - B. Wireless Communications
 - C. Wired Switch Port Access
 - D. IPSec Connections
 - E. VPN Connections

Correct Answer and Explanation: **B** and **C**. The 802.1x protocol integrates with network access equipment like wireless access points and infrastructure switches to provide port-level access control based on authorization from the NAP server.

Incorrect Answers and Explanations: **A**, **D**, and **E**. While these protocols are valid NAP connections, they cannot act as enforcement points for the 802.1x protocol since they all rely on established PPP transport methods or existing terminal connections.

4. You are troubleshooting a workstation that is not able to participate on the network because the NAP Agent isn't functioning correctly. Which fundamental communication will not occur until you restore the function of the NAP Agent?
 - A. Creation of the Statement of Health declarations
 - B. Creation of the System Statement of Health
 - C. Validation of the NAP policies
 - D. Creation of the Statement of Health Response

Correct Answer and Explanation: **B**. The NAP Agent is responsible for aggregating the individual SoH assertions into an overall System Statement of Health. Without this, the NAP process cannot be completed and the client is denied network access.

Incorrect Answers and Explanations: **A**, **C**, and **D**. While all of these are important to the function of the NAP infrastructure, these are not directly generated by the NAP Agent on the client workstation.

5. The NAP Health Registration Authority must be able to communicate with a number of different resources on your network to function correctly. Which services must be installed for the NAP HRA to participate on the network?
 - A. Active Directory
 - B. DHCP
 - C. NAP Administration Server
 - D. Certificate Authority

Correct Answer and Explanation: **C** and **D**. The HRA is responsible for mediating the communication between the NAP Administration Server and the enterprise PKI that is implemented to support the certificate exchanges in the NAP communication chain.

Incorrect Answers and Explanations: **A** and **B**. Both of these roles may be integral to the function of the corporate network, but are not in direct communication with the HRA.

6. You're planning to use the Windows System Health Agent (WSHA) as the primary SHA responsible for evaluating client health. You want to make sure that you have the appropriate resources available on the remediation network so workstations will be able to bring themselves into compliance. What resources might you want to make available to allow these machines to become compliant?

- A. The domain controller
- B. Windows Server Update Server (WSUS)
- C. Install files for Antivirus
- D. Certificate Authority

Correct Answer and Explanation: **B**, **C**, and **D**. All of these services directly support the workstation and can allow them to bring themselves into compliance through system patching, AV updates, and certificate enrollment, respectively.

Incorrect Answers and Explanations: **A**. A domain controller is certainly important for the authentication of the workstation, but is not usually a remediation server in itself.

7. You are an administrator of a corporate network and would like to configure a reliable and consistent environment for a training lab that will be based on thin-client workstations rather than complete workstations. Because you will be doing different kinds of training in the lab, it is important that these thin clients are able to easily adapt to the changing needs of the trainers. What kind of Terminal Services implementation would give the training staff the most flexibility when using this lab?

- A. Deploy a number of RemoteApp programs to match the training needs.
- B. Enable Remote Desktop for Administration.
- C. Configure Terminal Services Web Access.
- D. Configure Terminal Services with Vista Desktop.

Correct Answer and Explanation: **D**. In a lab environment, it is difficult to plan all of the different training needs in advance. It is important to give the training staff the most flexibility in the system configuration while helping to provide a credible workstation experience for the end user.

Incorrect Answers and Explanations: **A**, **B**, and **C**. None of these options would give the training lab the flexibility it would need to support a wide range of uses. Deploying individual applications would lead to administrative overhead and require IT support with every new configuration. Remote Desktop for Administration is only used for full Administrator connections and would not be appropriate. Web access, while possibly supporting the training environment, would not, in itself, enable the lab to function.

8. For the several months you have been running a network application over Terminal Services, it has become a core part of your business. Now that this application is considered to be mission-critical, what next steps should you take to ensure it is always available to the enterprise?
 - A. Implement RemoteApp to ensure the application is secure and to increase the stability of the server by isolating the application from the operating system.
 - B. Implement Session Broker and deploy additional terminal servers to provide a server farm with load balancing.
 - C. Implement Terminal Services Gateway to make the application available to the outside world and bring it into the scope of the corporate NAP authorization.
 - D. Implement Terminal Services Web Access to make the application available to remote users who may not have access to the RDP Client.

Correct Answer and Explanation: **B**. Deploying the session broker would allow multiple servers to be configured as a farm to support the mission-critical application, ensuring it is always available to end users.

Incorrect Answers and Explanations: **A**, **C**, and **D**. While these technologies might improve the presentation of this application to the clients, none of these directly improve the availability of the application.

9. Your terminal servers have suddenly stopped providing terminal connections to non-administrator clients trying to open terminal connections. What is the first thing you should check?
 - A. Check to be sure that the Terminal Services Licensing Service is running.
 - B. Ensure that the terminal server is running.
 - C. Restart the TS Broker Service.
 - D. Restart IIS to reset TS Web Access.

Correct Answer and Explanation: **A.** Since administrators can still connect, this indicates there is a problem with the licensing infrastructure since new clients aren't able to be authorized to make connections to the terminal servers.

Incorrect Answers and Explanations: **B, C, and D.** While all of these are important to the function of the terminal servers, they are not good starting points for the troubleshooting. Since administrators are able to connect, the issue lies farther up the chain from the physical server, but the licensing should be checked before moving on to the higher-level ancillary services.

10. Your company is planning to deploy a sales management system and would like to make this available to its traveling sales force as they move from client to client. You are planning to implement Terminal Services Client Access Licenses (TS CALs) in per-device mode. What is the downside of this choice?
 - A. The sales force will not be able to access the terminal server remotely.
 - B. Traveling agents will only be able to connect from corporate laptops.
 - C. The number of licenses purchased will have to match the number of remote sales agents.
 - D. You will not be able to load-balance connections through the TS Broker Service.

Correct Answer and Explanation: **B and C.** In per-device mode, the TS CALs will be bound to the physical workstations that the sales force will be using, requiring a 1:1 relationship between sales agents and licenses.

Incorrect Answers and Explanations: **A and D.** Even in per-device mode, sales agents will be able to access the terminal server remotely and through load-balanced connections as long as they have a valid TS CAL registered with the TS Licensing Service.

Chapter 3: Active Directory Forests and Domains

1. You are planning a Windows Server 2008 Active Directory infrastructure. You have a single location and there is a limited budget. During your planning process, you have determined that the members of the Domain Administrators group should have a password policy that states passwords must be changed every 24 days, and the rest of your users must change their passwords every 42 days, except for members of the Enterprise Admins group. These users must

change their passwords every 14 days. What is the best way to accomplish this without going over your budget, and keeping administration to a minimum?

- A. Create a single forest with three domains. In the forest root domain set a domain-wide password policy that states users must change their passwords every 14 days. Ensure all enterprise-wide administrators are placed into the Enterprise Admins group in the forest root domain. Create two child domains specifying the appropriate password policy in each domain.
- B. Create a single forest with two domains. In the forest root domain set a domain-wide password policy that states users must change their passwords every 14 days. Place all administrative users into the Enterprise Admins group in this domain, including those specified as Domain Admins. In the child domain, create a domain-wide password policy with the appropriate attributes and ensure only non-administrative users log on as users from this domain.
- C. Create a single-domain forest. Place all enterprise-wide users into the Enterprise Admins group, all domain administrators into the Domain Admins group, and all other users into the Users group. Create three password security objects (PSOs) with the appropriate attribute values set and deploy them to the appropriate security groups.
- D. Create a single-domain forest. Create three organizational units (OU), one for enterprise-wide administrators, one for domain administrators, and one for the rest of your users. Place all enterprise-wide users into the Enterprise Admins OU, all domain administrators into the Domain Admins OU, and all other users into the Users OU. Create three password security objects (PSOs) with the appropriate attribute values set and link them to the appropriate OU.

Correct Answers and Explanation: **C.** Password security objects are an advanced feature of Windows Server 2008, and allow you to set password policies and lockout policies to security groups within a domain.

Incorrect Answers and Explanation: **A and B** are incorrect because a single domain is all that is required in this scenario, and do not meet the security requirements stated. **D** is incorrect because PSOs can be applied to security groups, not OUs.

2. You are assessing the design of an Active Directory infrastructure for a company that has several business units. For legal reasons, these business units must remain separate entities each managing its own Active Directory infrastructure.

What would be the best design for this company, keeping their requirements in mind when creating the design?

- A. Create a single-domain forest, and place each business unit into its own organizational unit (OU).
- B. Create a single forest, and place each business unit into its own tree.
- C. Create a single forest and place each business unit into its own domain.
- D. Create a separate forest for each business unit.

Correct Answers and Explanation: **D**. This is correct because if each business unit needs to remain separate, then they should all have their own forest.

Incorrect Answers and Explanation: **A, B, C** are incorrect because these designs would not allow the business units to remain separate.

- 3. You have been hired to assess the installation of a Windows Server 2008 forest for a large company. The company will have nine business units, each using their own IT staff. For security and regulatory reasons, one of these business units must remain separate from the rest of the company. The other eight business units will need to have the ability to make their shared resources available to each other, in the need that a user from one business unit needs access to resources from another business unit. The other eight business units would also like to share a common global catalog (GC) database. Domain controllers from each business unit should not replicate user information to domain controllers outside of the business unit. How should you design Active Directory to meet the needs of this organization, with the least amount of administrative effort?
 - A. Create two forests. In one forest place the eight business units, each in their own domain. In the other forest place the other business unit. As the resource access needs arise, create Domain Local groups in the appropriate domain for giving permissions to the resources.
 - B. Create nine forests. For the eight business units that would like to allow access to each other's users to their resources, set up cross forest trusts. Set up connection objects in Active Directory Sites and Services to allow the GC in each forest to replicate with each other.
 - C. Create one forest. For the business unit that would like to remain separate, create its own tree. Place the other eight business units in the same tree of the forest.
 - D. Create two forests. In one forest place the eight business units, each into their own Organizational Unit (OU). Place all user, computer and domain

controller objects into the appropriate OU. In the other forest, place the other business unit.

Correct Answers and Explanation: **A**. Because the one business unit needs to remain totally separate, it should be placed into its own forest. The other eight units all wish to share a GC and therefore need to be placed into a single forest, and since they all have their own IT staff should have their own domains as well.

Incorrect Answers and Explanation: **B** is incorrect because placing the other eight units into separate forests will not allow them to share a GC. **C** is incorrect because the one unit needs to remain separate and therefore should be in its own forest. **D** is incorrect because a single domain will not allow each unit's IT staff to separate themselves from each other.

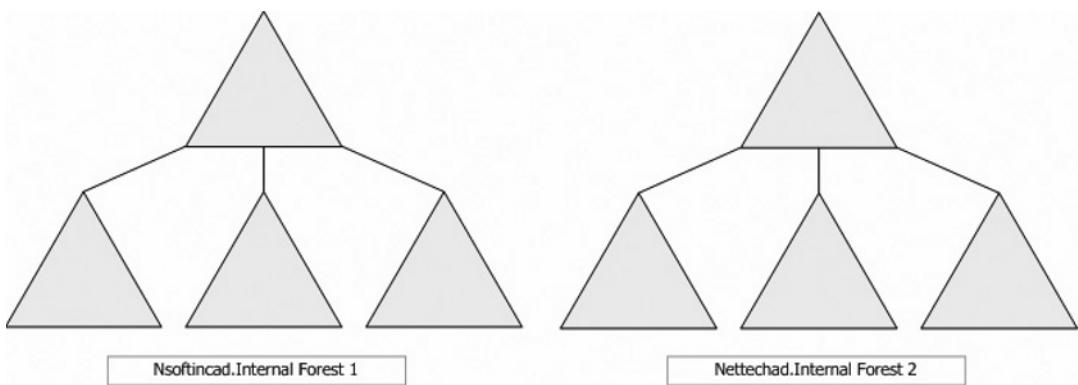
4. You have been asked to help design the Active Directory infrastructure for a large organization. One department in this company will be installing an application that will make several modifications to the Active Directory schema. The rest of the company must not see those schema modifications. However, there will be some resources that will be shared by all departments. What is the best way to design this company so that only the department using the application can see the schema modifications?
 - A. Create a single forest with two trees. In the first tree, place all of the departments that do not need this specialized application into their own domains. In the second tree, place the department that uses this specialized application into its own domain. Transfer the schema master to the domain controller in the second tree and make the modifications to the schema.
 - B. Create a single forest with two trees. In first tree, place the one department that needs the application. Modify the schema on the schema master. Then create the other tree and add the rest of the departments to the domain in the second tree.
 - C. Create two forests each with a single domain. In the first forest add the department that uses the specialized application and modify the schema. In the second forest place the rest of the departments. Create a cross-forest trust between the two forests.
 - D. Create two forests each with a single domain. In the first forest add the department that uses the specialized application and modify the schema. In the second forest place the rest of the departments. Ensure **Bridge all site links** has been enabled for both forests.

Correct Answers and Explanation: **C.** Schema modifications affect the entire forest, therefore you need to create two forests; one for the one department and one for the rest of the company. You also need to create a trust between the forests to allow each department to share resources.

Incorrect Answers and Explanation: **A and B** are incorrect because we need two forests. **D** is incorrect because the option **Bridge all site links** will not allow users from both forests to share resources.

5. You have designed the Active Directory infrastructure for a company that has two forests, each with four domains (as shown in Figure 3.16). You are doing an inventory of all of the domain controllers and the operations master tokens they hold. How many of each should you expect to find?

Figure 3.16 AD Infrastructure with Two Forests and Four Domains



- A. 2 Schema, 2 Domain Naming, 8 Infrastructure Master, 8 PDC Emulator, 8 RID Master
- B. 8 Schema, 8 Domain Naming, 8 Infrastructure Master, 8 PDC Emulator, 8 RID Master
- C. 2 Schema, 2 Domain Naming, 8 Infrastructure Master, 8 PDC Emulator, 8 RID Master
- D. 8 Schema, 8 Domain Naming, 2 Infrastructure Master, 2 PDC Emulator, 2 RID Master

Correct Answers and Explanation: **A.** The operations master roles are divided into forest wide and domain-wide. The forest-wide roles are the schema master and domain naming master. This means that each forest, regardless how many domains have been created in the forest, will have only one schema master and one domain naming master. The domain wide roles are the PDC emulator, RID master and the infrastructure master. Each domain, including the forest root domain will have one of each. In this scenario there are two forests with a total of eight domains.

Incorrect Answers and Explanation: **B, C, D.** These are incorrect because there are two forests, therefore 2 schema masters and 2 domain naming masters, and 8 domains, so 8 PDC emulators, 8 RID masters, and 8 infrastructure masters.

6. You have been asked to assist in the upgrade of a single-domain forest from Windows Server 2003 to Windows Server 2008. Currently all DCs in all domains run Windows Server 2003. You decide to upgrade the DCs to Windows Server 2008 as an in-place upgrade. However, the company is running an application that must reside on DC running Windows Server 2003, so you decide that it would be best to keep that DC running Windows Server 2003 until the application vendor upgrades the application. What is the best way to upgrade this forest, while keeping the application running?
 - A. Upgrade the first DC to Windows Server 2008. Make sure the forest function level and domain function level remain at Windows Server 2003. When the application gets upgraded, upgrade the final domain controller and then raise the forest function level to Windows Server 2008.
 - B. Upgrade the first DC to Windows Server 2008. Raise the forest function level to Windows Server 2008 but keep the domain function level at Windows Server 2003. When the application gets upgraded, raise the domain function level to Windows Server 2008.
 - C. Uninstall the application. Upgrade all DCs to Windows Server 2008. Raise the forest and domain function levels to Windows Server 2008. Install Windows Server 2003 on a member server and then run **dcpromo.exe** to install Active Directory on the member server, as a Replica Domain Controller for an existing Domain. Reinstall the application on the Windows Server 2003 DC.

- D. Uninstall the application. Upgrade all DCs to Windows Server 2008, except for the DC that held the application. Move the Windows Server 2003 DC into its own Organizational Unit (OU). Raise the forest and domain function levels to Windows Server 2008. Reinstall the application.

Correct Answers and Explanation: **A**. Because one DC must remain at Windows Server 2003, you cannot raise the domain function level to Windows Server 2008.

Incorrect Answers and Explanation: **B** is incorrect because you cannot have a Windows Server 2008 forest function level while having a Windows Server 2003 domain function level. **C and D** are incorrect because uninstalling the application will not keep it running, and the domain and forest function levels must remain at Windows Server 2003 while the DC is still running Windows Server 2003.

7. You have been asked to provide a domain controller to a branch office. The office has 200 users, but no IT staff on site. One user in the branch office is competent enough that, if you needed him to do something with the Domain Controller, he would be able to assist with little help. Also, due to the layout of the office, there is no room in which to lock the server to provide physical security. What should you do to provide the branch location with a Domain Controller while not compromising security?

- A. Provide a DC to the branch and transfer the infrastructure master role to the DC. Add the competent user to the Domain Admins group.
- B. Provide a DC to the branch and transfer the RID master role to the DC. Add the competent user to the Domain Admins group.
- C. Provide a read-only domain controller (RODC) to the branch office and add the competent user to the Domain Admins group.
- D. Provide a read-only domain controller (RODC) to the branch office and make the competent user a local administrator on the RODC.

Correct Answers and Explanation: **D**. Read-only domain controllers (RODCs) are a new type of DC in Windows Server 2008. These DCs have a read-only database and allow for administrator separation, or the ability to have a user be an administrator on the RODC without giving domain-wide administrative rights.

Incorrect Answers and Explanation: **A and B** are incorrect because these DCs are writeable and should not be left in an un-secure location. Also adding the

user to the Domain Admins group will compromise security. **C** is incorrect because adding the user to the Domain Admins group will compromise security.

8. You are planning the upgrade of your Windows Server 2003 Active Directory infrastructure to Windows Server 2008. What must you do before introducing the first Domain Controller running Windows Server 2008?
 - A. Install Windows Server 2008 on a member server and join it to the domain. Add the computer object to the Domain Controller's Global Security group.
 - B. Install Windows Server 2008 on a member server and join it to the domain. Move the computer object to the Domain Controller's organization unit (OU).
 - C. On the schema master run **adprep /forestprep**.
 - D. On the schema master run **regsvr32 schmmgmt.dll**.

Correct Answers and Explanation: **C**. Before installing Windows Server 2008 and Active Directory in your Windows Server 2003 environment, you should run adprep /forestprep to prepare the forest for the new schema attributes introduced in Windows Server 2003.

Incorrect Answers and Explanation: **A** is incorrect because you would need to run adprep /forest prep prior to installing AD DS. Joining a member server to the Domain Controllers global security group is not a good idea. **B** is incorrect because you need to run adprep /forestprep. Adding this member server to the Domain Controllers OU is not a good idea. **D** is incorrect because running this command will make Active Directory Schema an available snap-in but will not prepare the schema for Windows Server 2008.

9. You have been asked to assess the effect of an application in Active Directory. The application will add schema attributes, when installed. Your Active Directory forest is running at Windows Server 2008 forest function level. After testing the application you decide not to implement it. After you uninstall the application, you notice that the schema attributes which were added at installation are still present. You need to remove the effects of these attributes on Active Directory.
 - A. Open Active Directory Schema. Browse through the attributes until you find the attributes you need to remove. Click the attribute, and on your keyboard press **Delete**.

- B. Open Active Directory Schema. In the Properties of the attribute, select **Index this attribute**.
- C. Open Active Directory Schema. In the Properties of the attribute deselect the attribute that is active.
- D. Open Active Directory Schema. In the Properties of the attribute, in the **Syntax and Range** field, set both **Minimum** and **Maximum** values to **0**.

Correct Answers and Explanation: **C**. You cannot delete a schema attribute which has been added, you can only de-activate it.

Incorrect Answers and Explanation: **A** is incorrect because you cannot delete a schema attribute. **B** is incorrect because indexing the schema attribute will not de-activate it. **D** is incorrect because setting these values to 0 will not deactivate the attribute, it will make the attribute have no value, but the attribute itself will still be there.

- 10. You are designing the Active Directory deployment of Windows Server 2008 Active Directory for a large organization with several branch offices. What are some factors to consider when deciding whether to use a read-only domain controller (RODC) as your only DC at a branch office location? Choose two answers to complete the solution.
 - A. An RODC cannot hold the operations master tokens
 - B. An RODC should hold all operations master tokens
 - C. An RODC cannot hold the bridgehead server role
 - D. An RODC should hold the bridgehead server role

Correct answers: **A and C**. A is correct because your RODC cannot hold the operation master roles. If the DC that gets placed in the branch office were required to hold one of these roles, then you could not use an RODC. C is correct because the RODC cannot be a bridgehead server, which would be required if the branch office were its own Site.

Incorrect Answers and Explanation: **B and D** are incorrect because the RODC cannot be an operations master or a bridgehead server.

Chapter 4: Designing an Enterprise-Level Group Policy Strategy

- 1. You are the Group Policy administrator for your company. The users in your accounting department need to have a custom application installed. You have

contacted the vendor and they have supplied you with an MSI installation file. All of the users in your accounting department and their computer objects are in the Accounting OU. Each member must decide when the application gets installed. For security purposes, you do not allow these users to access Control Panel. How should you configure the Group Policy?

- A. Link the GPO to the Accounting OU. Publish the Application to the Users group.
- B. Link the GPO to the Accounting OU. Assign the Application to the Users group.
- C. Link the GPO to the Accounting OU. Assign the Application to the Computers group.
- D. Link the GPO to the Accounting OU. Assign a startup script that will install the application to the Computers group.

Correct Answer: **B.** Because the users must decide when the application gets installed, it must be configured under User Configuration. By assigning the application, it will show up on the **Start** menu, but not install until a user launches it.

Incorrect Answers: **A, C, D.** **A** is incorrect because the users cannot access the Control Panel; therefore you should not publish the application. **C** and **D** are incorrect because the application needs to be configured for the Users group, not the Computers group.

2. You are the Group Policy administrator for your company. All of the user accounts get created in the Users container and then get moved into their appropriate containers. You need to ensure that upon the creation of a new user account, it immediately receives a GPO called New Employee GPO; but other employees do not receive the settings from this GPO. How should you configure your environment?
 - A. Create an OU called New_Employees. Create a GPO called New Employees GPO and link it to the New_Employees OU. Run the **redirusr** command to redirect all new user accounts to the New_Employees OU.
 - B. Create an OU called New_Employees. Create a GPO called New Employees GPO and link it to the New_Employees OU. Run the **redircmp** command to redirect all new computer accounts to the New_Employees OU.

- C. Create an OU called New-Employees. Create a GPO called New Employees GPO and link it to the domain. In the attributes of the GPO, select **Enforced**.
- D. Create a GPO called New Employees GPO. Create a global security group called New Employees. Add all new employees to the global security group. In the Delegation tab of the GPO, accept all default entries and then add New Employees security group with the Apply group policy permission set to **Allow**. Link the GPO to the domain.

Correct Answer: **A.** **A** is the correct answer. **Redirusr** is a command that will redirect the user accounts to an OU you specify when they are created by a method that does not specify the OU. Because the default location is a container and not an OU, the only way to get a GPO applied is to link it to the domain. In this question, the GPO cannot be linked to a domain.

Incorrect Answers; **B, C, D.** **B** is incorrect because you must run **redirusr**, not **redircmp**. **C** is incorrect because the GPO cannot be linked to the domain since the question states that other users should not get the GPO. **D** is incorrect because other users would also get this GPO applied since the default security is Authenticated Users have Read and Apply group policy permissions.

- 3. You have been asked to create a Group Policy Object to be used as a template for other Group Policy Objects. What is the best way to create this GPO with the least amount of administrative effort?
 - A. Create a GPO and configure all appropriate settings. Use the GPMC to create an HTML report of the settings. For each new GPO, refer to this HTML report and reconfigure these same settings.
 - B. Create a GPO and configure all appropriate settings. Use GPMC to back up the GPO. For each new GPO, start by restoring the GPO and continuing from there.
 - C. Create a Starter GPO and configure all appropriate settings. For each new GPO, select the Starter GPO.
 - D. Create an Administrative Template (ADMX file). For each new GPO, import the ADMX file into the new GPO.

Correct Answer: **C.** **C** is the correct answer. Starter GPOs are GPOs that you configure and use as templates for creating other GPOs that begin with these same settings.

Incorrect Answers: **A, B, D.** **A** is incorrect because even though this will work, it is a lot of effort and leaves a lot of margin for error. **B** is incorrect because restoring the GPO is not a way to create a new GPO; however, it will restore an existing GPO to the state of the backup. **D** is incorrect because Administrative Templates are sections within the GPO. They will not allow you to create a new GPO with existing settings.

4. You are the Group Policy administrator for your company. Your company has a single forest with three domains, located in the U.S. and Canada. The company is headquartered in Toronto and has members from all domains in the Toronto office. You have been asked to create a Group Policy Object that will apply to only the computers in the Toronto location. You have ensured that your user account is in the Enterprise Admins group, as well as the Domain Admins group is in the forest root domain. How should you configure this GPO?
 - A. Create a GPO with the required settings and link it to the Toronto site.
 - B. Create a GPO with the required settings and link it to all of the domains.
 - C. Create a GPO with the required settings and link it to the Domain Controllers OU in the forest root domain.
 - D. Create a GPO with the required settings and link it to the Domain Controllers OU in each of the domains.

Correct Answer: **A.** **A** is the correct answer because you need to link the GPO to the Toronto site to allow it to apply to all computers that are within the IP boundaries of Toronto regardless of their domain.

Incorrect Answers: **B, C, D.** **B** is incorrect because the GPO would apply to all computers, not just those in Toronto. **C** is incorrect because the GPO would apply only to the DCs in the forest root domain. **D** is incorrect because the GPO would apply only to the DCs in all of the domains.

5. You are the Group Policy administrator for your company. Your company has locations throughout the U.S. and Canada and is setup as a single domain. You want to ensure that Group Policies can be created by administrators in each geographic location and processed by the clients in each location without requiring the sending of traffic over the WAN. Which Administrative Template setting should you configure?
 - A. Computer Configuration-Group Policy Slow Link Detection, enabled to 500Kbps.

- B. User Configuration-Group Policy Slow Link Detection, enabled to 500Kbps.
- C. Computer Configuration-Environment Policy Processing, enabled to **Allow processing across a slow network connection.**
- D. User Configuration-Group Policy Domain Controller Selection.

Correct Answer: **D.** The settings **User Configuration | Policies | Administrative Templates | System | Group Policy | Group Policy Domain Controller Selection** can be configured to choose any writeable DC instead of the default PDC Emulator.

Incorrect Answers: **A, B, C.** **A** is incorrect because this will set the threshold to what Group Policy considers a slow link when applying Computer Configuration settings. It has nothing to do with the DC selection. **B** is incorrect because it will set the threshold to what Group Policy considers a slow link when applying User Configuration settings. **C** is incorrect because it simply tells Group Policy to process Environment Policies over a slow link.

- 6. You have just logged onto your workstation and noticed several policies that have been applied. You want to see which policies have been applied and then save the report as HTML. What are two ways to accomplish this? (Choose two answers. Each answer represents a complete solution.)
 - A. Use **gpresult /R /H** and add the path to where you want to save the report.
 - B. Use the GPMC and Group Policy Modeling Wizard.
 - C. Use the GPMC and Group Policy Results Wizard.
 - D. Use **gpupdate /force >c:\gpo.htm**.

Correct Answers: **A** and **C.** **A** is correct because **gpresult** is a command-line tool that will allow you to see what settings have been applied. **/R** tells **gpresult** to run a results report and **/H** tells **gpresult** to format that report in HTML. **C** is right because GPMC comes with a Group Policy Results Wizard which will automatically display the report in HTML.

Incorrect Answers: **B, D.** **B** is incorrect because the Group Policy Modeling Wizard will show what will happen if a user logs onto a computer instead of what did happen. **D** is incorrect because **gpupdate** tells your workstation to request Group Policy updates. By piping in a path, the success or failure message from the update process will be written as an HTML report, not as the settings that were applied.

7. You are the Group Policy administrator for your domain and have been tasked with creating a policy that will apply to all of the computers in your domain, except for those computers in the Accounting OU, and including the computers in the Computers container. The computers in the Accounting OU should still receive all of the settings from the Default Domain Policy. How can you design your Group Policy infrastructure to allow the GPO to apply to all computers except for those in the Accounting OU while allowing the settings from the Default Domain Policy to apply to the specified computers?
- A. Link the new GPO to each of the OUs except for the Accounting OU. On the Default Domain Policy, select **Enforced**.
 - B. Link the new GPO to the Accounting OU. On the Accounting OU, select **Block Inheritance**. On the Default Domain Policy, select **Enforced**.
 - C. Link the new GPO to the domain. On the Accounting OU, select **Block Inheritance**. On the Default Domain Policy, ensure Authenticated Users have **Read** and **Apply** group policy permissions.
 - D. Link the new GPO to the domain. On the Accounting OU, select **Block Inheritance**. On the Default Domain Policy, select **Enforced**.

Correct Answer: **D.** **D** is correct because you must link the new GPO to the domain to ensure it applies to all computers. You must also **Block Inheritance** on the Accounting OU to ensure that no policies from the domain are applied on these computers unless the **Enforced** attribute is selected. Therefore, you must select **Enforced** on the Default Domain Policy.

Incorrect Answers: **A, B, C.** **A** is incorrect because the computers in the Computers container will not get this new policy. **B** is incorrect because this policy should be linked to the domain, not the Accounting OU. **C** is incorrect because you need to select **Enforced** on the Default Domain Policy.

8. You are the administrator of a Windows Server 2008 Active Directory forest. You have a single domain in a single location. You want to use scripting to manage your Group Policy Objects, including creating new objects, backing up and restoring GPOs, and creating reports for the GPOs. What tool should you use for this?
- A. Windows Command Prompt. Use **gpresult.exe**.
 - B. Windows Command Prompt. Use **gpupdate.exe**.
 - C. Windows PowerShell.
 - D. Group Policy startup scripts.

Correct Answer: C. Windows PowerShell is a powerful scripting tool that will allow you to manage GPOs from the PowerShell command window.

Incorrect Answers: **A, B, D.** **A** is incorrect because **gpresult** will not allow you to manage GPOs. **B** is incorrect because **gpupdate** will not allow you to back up GPOs. **D** is incorrect because startup scripts are elements inside GPOs. They will not allow you to manage GPOs.

9. You are the administrator for your company's Windows Server 2008 Active Directory domain. You have designed the OU infrastructure so that each department has its own OU, with a child OU for the Users group and another child OU for the Computers group, with the appropriate objects placed into the appropriate OUs. You have decided to let the department managers link GPOs to their OUs as they feel are necessary. What should you do to allow the department managers to link the GPOs to their own OUs without allowing them to link GPOs to other OUs?
 - A. Use the Delegation of Control Wizard on each OU. Delegate Generate Resultant Set of Policy (Planning) to the department managers.
 - B. Use the Delegation of Control Wizard on each OU. Delegate Generate Resultant Set of Policy (Logging) to the department managers.
 - C. Use the Delegation of Control Wizard at the domain. Delegate Manage Group Policy links to the department managers.
 - D. Use the Delegation of Control Wizard at each OU. Delegate Manage Group Policy links to the department managers.

Correct Answer: **D.** **D** is the correct answer because you need to use the Delegation of Control Wizard at the OU and delegate **Manage group policy links**. This will allow the department managers to link, unlink, and set **Enforced** and **Block Inheritance** at their OU.

Incorrect Answers: **A, B, C.** **A** and **B** are incorrect because these are the wrong tasks to delegate. **C** is incorrect because this task should be delegated at the OU. Delegating at the domain will give department managers more control than required in the question.

10. You are the Group Policy administrator for your company's Active Directory domain. You have been assigned the task of creating a Standard Desktop for users in the sales department, which are spread throughout the U.S. and Canada. These users must all have the same security settings and applications installed on their desktops. These applications should only get installed on

the computers in the sales department. What is the most efficient method for achieving this?

- A. Put all users from the sales department into the same OU. Create and link a GPO to this OU that will configure all of the settings and install the appropriate applications. Mark the GPO as **Enforced**.
- B. Put all users from the sales department into the Users container. Create and link a GPO to the domain that will configure all of the settings and install the appropriate applications. Mark the GPO as **Enforced**.
- C. Put all users from the sales department into the same IP subnet. Create and link a GPO to the site containing this IP subnet that will configure all of the settings and install the appropriate applications.
- D. Put all users from the sales department into the same OU. Create and link a GPO to the domain that will configure all of the settings and install the appropriate applications. Ensure the users from the sales department have Read and Apply group policy permissions. Configure the OU to **Block Inheritance**.

Correct Answer: **A.** **A** is correct because adding all users into the same OU and linking to that OU is the most efficient way to achieve your goal. Marking the GPO as **Enforced** ensures that the settings will apply even if a conflicting GPO gets added.

Incorrect Answers: **B, C, D.** **B** is incorrect because these users should be in the same OU, not the Users container. **C** is incorrect because these users are spread out over the U.S. and Canada, and it is not practical to add them to the same IP subnet. **D** is incorrect because linking the GPO to the domain means it will apply to many users, not just the appropriate users. And marking the OU as **Block Inheritance** means the policy will not apply to those users.

Chapter 5: Designing Identity and Access Management

1. You want to upgrade your existing infrastructure to Windows Server 2008. Which factors should influence your upgrade?
 - A. Time constraints
 - B. Resource availability
 - C. Budget
 - D. Application compatibility

Correct Answers and Explanations: **A**, **B**, **C** and **D**. All answers are correct because all of these factors influence the design and planning of an upgrade.

2. Simon is in the process of an intra-forest restructuring of his Active Directory. He wants to maintain user passwords during the migration. For this purpose he installs the PES service on one of the domain controllers in the source domain. When he selects the **Migrate passwords** option in ADMT and clicks **next**, an error occurs stating that PES service cannot be contacted in the source domain. What could be the cause for this error? (Select all that apply)
 - A. Password migration is not supported in an intra-forest migration.
 - B. He didn't install the PES Service on the PDC Emulator FSMO role holder.
 - C. He didn't set the **AllowPasswordExport** Registry value to **1** on the PES.
 - D. He must be a member of the **AllowPasswordExport** group in the source domain.

Correct Answers and Explanations: **B** and **C**. Answer **B** is correct, because the PES must be installed on the PDC Emulator. Answer **C** is correct because the **AllowPasswordExport** Registry value must be set to **1** to allow password migration.

Incorrect Answers and Explanations: **A** and **D**. Answer **A** is incorrect because password migration is supported in an intra-forest scenario. Answer **D** is incorrect because the group **AllowPasswordExport** does not exist and is not needed for password migration.

3. You decided to install a new Windows Server 2008 domain controller into your existing Windows Server 2003 Active Directory. What tasks do you have to complete before installing the first Windows Server 2008 Domain Controller?
 - A. Raise the forest functional level to Windows Server 2003
 - B. Extend the Active Directory Schema
 - C. Prepare the Domain
 - D. Pre-stage the Domain Controller account in Active Directory

Correct Answers and Explanations: **B** and **C**. Answers **B** and **C** are correct because you need to extend the schema and prepare the AD domain to be able to install a Win2008 DC.

Incorrect Answers and Explanations: **A** and **D**. Answer **A** is incorrect because the minimum requirement for installation of a Win2008 DC is Windows 2000 Native Mode. Answer **D** is incorrect, because there's no way of pre-staging a DC account. Furthermore, this is not needed.

4. Your company is operating a Windows Server 2008 Active Directory. The Forest is operating at Windows Server 2008 functionality level. Your boss tells you to install an additional Windows Server 2003 domain controller into the domain because of some application compatibility issues. When you try to install the new domain controller, you fail. What could be the reason for your failure?
 - A. You didn't use the **/adv** switch when running DCPROMO.
 - B. You cannot add Windows Server 2003 domain controllers to a forest that is operating at Windows Server 2008 functionality mode.
 - C. Your Windows Server 2003 domain controller is not running Service Pack 2.
 - D. You didn't enable the Windows Server 2003 compatibility flag on the domain where you try to install the new domain controller.

Correct Answers and Explanations: **B**. Answer **B** is correct and is self-explanatory.

Incorrect Answers and Explanations: **A**, **C**, and **D**. Answer **A** is incorrect because the **/adv** switch is used to install a DC from media. Answer **C** is incorrect because Win 2003 Service Pack 2 does not change anything. Answer **D** is incorrect because there is no such flag that you can set.

5. Mark is in the middle of a migration to a new Active Directory Forest. Recently he migrated the first bulk of users by using ADMT. However, when users log on with the new account, they cannot access resources in the old forest. He examines the user accounts in Active Directory and discovers that the SID History is correctly populated. What else must he do to allow resource access with SID History?
 - A. Enable the **use SID History** flag in the source forest.
 - B. On the target forest, disable SID Filtering on the incoming trust.
 - C. Add the new user accounts to the access control list on servers in the source forest.
 - D. On the Source Forest, disable SID Filtering on the incoming trust.

Correct Answers and Explanations: **D.** Answer **D** is correct because SID Filtering is enabled by default on Trust in Windows Server 2003 and 2008. The incoming trust in the source forest must be used because a user from the target forest needs to access resources in the source forest. Therefore the user is incoming.

Incorrect Answers and Explanations: **A, B, C.** Answer **A** is incorrect because the flag **use SID History** does not exist. Answer **B** is incorrect because if you disable SID Filtering on the incoming trust of the target forest it would have no effect on a user from the target forest accessing resources in the source forest. Answer **C** is incorrect because this solution would work but would omit SID History.

6. Linda is migrating Users and Groups to a new forest using ADMT. After she migrates all of her user accounts, she discovers that the group membership is empty. What steps must she take before she migrates user accounts?
 - A. Migrate groups first.
 - B. Export the group membership on the source forest and then import it on the target forest.
 - C. Select the **preserve group membership** checkbox in ADMT.
 - D. Do nothing, as this is by design.
7. Your company is restructuring the existing Active Directory. You want to install the Password Export Server (PES) Service on a domain controller in a source domain. You run the **admt /key** command to create the PES key. When you install PES, an error occurs stating that the key is not valid for this domain. What can be the cause for this error?
 - A. PES cannot be used for Intra-Forest restructuring.
 - B. PES must be installed in the target domain.

- C. You must use a stronger encryption algorithm for the key.
- D. The PES key must be created in the target domain.

Correct Answers and Explanations: **D**. Answer **D** is correct because the PES key must be created in the target domain and then be transferred to the source domain.

Incorrect Answers and Explanations: **A**, **B**, and **C**. Answer **A** is incorrect because ADMT definitely supports intra-forest restructuring. Answer **B** is incorrect because PES must be installed in the source domain to extract and copy passwords. Answer **C** is incorrect because the algorithm used to encrypt the PES key is fixed.

8. Alan wants to restructure his Windows Server 2003 Active Directory Forest. He decided to build a new forest. The forest is operating at Windows Server 2008 forest functionality level. He uses ADMT Version 3 to migrate users, groups, and computers. When he starts with the group migration, ADMT fails to migrate accounts. Why isn't he able to migrate accounts?
 - A. Migration between Windows Server 2003 and Windows Server 2008 is not supported.
 - B. He must use the version of ADMT specifically built for Windows Server 2008.
 - C. He must install at least one Windows Server 2008 domain controller in the source forest.
 - D. If you use ADMT Version 3, the target forest must not operate at Windows Server 2008 Forest functionality level and at least one Windows Server 2003 domain controller must be present.

Correct Answers and Explanations: **B** and **D**. Answer **B** is correct because ADMT Version 3 is not compatible with a forest that is running Windows Server 2008 domain controllers only. Answer **D** is correct because the target forest is not allowed to operate at Windows Server 2008 functionality mode if you use ADMT Version 3.

Incorrect Answers and Explanations: **A**, **C**, and **D**. Answers **A** is incorrect because it is possible to migrate from forests that are operating at Windows 2000 Native mode or Windows server 2003 mode. Answer **C** is incorrect because installation of a Windows Server 2008 domain controller in the source forest is not necessary to migrate accounts to a Windows Server 2008 forest.

9. Your boss tells you to use the Microsoft Solutions Framework (MSF) to manage your migration project. Which of the following phases are recommended by MSF?
- A. Envisioning
 - B. Strategy
 - C. Stabilizing
 - D. Deployment
 - E. Managing

Correct Answers and Explanations: **A**, **C**, and **D**. Answers **A**, **C**, and **D** are correct because they are part of the MSF framework.

Incorrect Answers and Explanations: **B** and **E**. Answers **B** and **E** are incorrect because they are not part of MSF.

10. Which of the following protocols does Web Services use?
- A. XML
 - B. SOAP
 - C. IPSEC
 - D. HTTP

Correct Answers and Explanations: **A**, **B**, and **D**. Answers **A**, **B**, and **D** are correct, because WS relies on those protocols to provide its functionality.

Incorrect Answers and Explanations: **C**. Answer **C** is incorrect because Web Services does not rely on IPSEC to work correctly.

Chapter 6: Designing a Branch Office Deployment

1. You have been asked to design a branch office deployment for your company. Which of the following might influence your design?
- A. User population
 - B. WAN link availability
 - C. Physical security
 - D. Technical on-site expertise

Correct Answers and Explanations: **A, B, C, D.** Answers **A, B, C** and **D** are correct because they all influence the design of a branch office deployment.

2. Your company is implementing Read-only Domain Controllers. You install a Windows Server 2008 domain controller in your domain to support installation of RODCs. Which FSMO role should you assign to this domain controller?
 - A. RID master
 - B. Infrastructure master
 - C. Schema master
 - D. PDC emulator
 - E. Domain naming master

Correct Answer and Explanation: **D.** Answer **D** is correct because the PDC Emulator is used to create special **krbtgt** accounts for RODCs.

Incorrect Answers and Explanations: **A, B, C, E.** Answers **A, B, C**, and **E** are incorrect because these roles don't have any effect on the installation of an RODC.

3. Alice works as a system administrator at a company called Wiredworld. She wants to prepare Active Directory for RODC operation. Which steps does she need to take to prepare Active Directory for RODC operation?
 - A. Raise the Forest functionality level to Windows Server 2003
 - B. Raise the Domain functionality level to Windows Server 2008
 - C. Prepare Active Directory by running adprep/rodcprep
 - D. Transfer the PDC Emulator FSMO role to a Windows Server 2008 domain controller

Correct Answers and Explanations: **A, C, D.** Answer **A** is correct because RODC is dependent in linked-value replication, which is only available in Windows Server 2003 Forest Functionality Level. Answer **C** is correct because permission needs to be upgraded on DNS zones in AD for RODC operation. Answer **D** is correct because the PDC Emulator is used to create the special **krbtgt** account for RODCs.

Incorrect Answer and Explanation: **B.** Answer **B** is incorrect because Windows Server 2008 Domain Functionality Level is not required to install an RODC.

4. As a branch office administrator, you have been asked to complete the installation of a prestaged Read-only domain controller on a server core machine. Which command would you use to start the installation?
- A. dcpromo /AttachAccount
 - B. dcpromo /InstallPrestagedAccount
 - C. dcpromo /UseExistingAccount:Attach
 - D. dcpromo /CompletePrestaging
- Correct Answer and Explanation: **C.** Answer **C** is correct because it uses the correct command.
- Incorrect Answers and Explanations: **A, B, D.** Answer **A, B**, and **D** are not correct because each answer uses an incorrect command line switch.
5. Bart is a systems administrator at xxx. The network consists of several sites in which RODCs are deployed. Bart wants to prepopulate passwords for users that must be authenticated on all RODCs at all times. He creates a new group and adds the required users as members. After that, he adds a new allow entry for the group to every RODC. A few minutes later, he tries to prepopulate users' passwords and receives an error. What else must he do to be able to prepopulate the users' passwords?
- A. Add an individual allow entry for every user
 - B. Initiate Active Directory replication
 - C. Add the allow entry directly on the RODC
 - D. Wait for replication to finish
- Correct Answers and Explanations: **B, D.** Answer **B** is correct because after you add an allow entry to the password replication policy, the new policy settings need to replicate to all RODCs to allow prepopulation of passwords. Answer **D** is correct because Bart could simply wait for normal ad replication to complete.
- Incorrect Answers and Explanations: **A, C.** Answer **A** is incorrect because adding an individual entry for every user would not help in this situation. Password Replication Policies support the use of groups. Answer **C** is incorrect because adding an entry directly on the RODC is not possible because it is read-only.
6. James is a Systems administrator for an Active Directory environment. The domain functional level is Windows Server 2008. John wants to enable Active

Directory backup for BitLocker and TPM modules. Which steps does he need to take? (choose all that apply)

- A. Extend the Active Directory schema
- B. Add permissions on the domain container
- C. Add users to the “Allow BitLocker Backup” Group in Active Directory
- D. Configure Group Policy settings for BitLocker and TPM Active Directory backup

Correct Answers and Explanations: **A, B, D.** Answer **A** is correct because Active Directory needs to be extended to enable storage of BitLocker recovery information. Answer **B** is correct because you need to assign Permission on the domain container to allow computers to store TPM recovery information. Answer **D** is correct because you need to enable BitLocker Active Directory backup for clients via Group Policy.

Incorrect Answer and Explanation: **C.** Answer **C** is incorrect because you do not need to add users to a group to be able to back up BitLocker information in AD. The computer does this. The group “Allow BitLocker Backup” does not exist.

7. You are the systems administrator of an Active Directory domain. All Servers are running Windows Server 2008 and have TPM compatible hardware. Your company security policy has been updated recently and requires BitLocker drive encryption all server machines. When you want to enable BitLocker on the first server you receive a warning that the drive configuration is unsuitable for BitLocker drive encryption. What options do you have?
- A. Shrink the operating system partition, create a new partition, activate the new partition, and copy the boot configuration store to the new partition.
 - B. Install the operating system from scratch. Before you start the installation, create the correct partitioning scheme.
 - C. Use the BitLocker Drive Preparation Tool.
 - D. Configure BitLocker to use a USB drive for encryption.

Correct Answer and Explanation: **B.** Answer **B** is correct because on Windows Server 2008 the drive configuration cannot be changed without reinstalling the operating system.

Incorrect Answers and Explanations: **A, C, D.** Answer **A** is incorrect because by activating the new partition, the system would be unbootable, since there is no

boot sector on the partition. Answer **C** is incorrect because the tool is available for download only on Windows Vista Ultimate and Enterprise. Answer **D** is incorrect because USB drives cannot be used for encryption, only for startup key storage.

8. What components are validated by BitLocker boot integrity check?
 - A. Master Boot Record
 - B. BIOS
 - C. Boot Configuration Data Store
 - D. Boot Manager Code
 - E. Boot Sector

Correct Answers and Explanations: **A, B, D, E**. Answers **A, B, D**, and **E** are correct because they are checked by the TPM.

Incorrect Answer and Explanation: **C**. Answer **C** is incorrect because the Boot Configuration Data store is encrypted on disk and cannot be read by the integrity check.

9. You replace the motherboard of a BitLocker protected computer. When you turn on the computer, the system is locked and does not boot. Which precautions do you have to take in order to replace the motherboard on a BitLocker protected system while keeping data secured?
 - A. Decrypt all protected volumes in Control Panel
 - B. Disable BitLocker in Control Panel
 - C. Remove the TPM module from the old motherboard and plug it into the new motherboard.
 - D. Save the current startup integrity checksum on a USB drive and restore it on the new system.

Correct Answer and Explanation: **B**. Answer **B** is correct because when you disable BitLocker, data is kept encrypted on the disk. The volume master key is encrypted with a new key, which is stored unencrypted on the disk, therefore making the disk readable on another system.

Incorrect Answers and Explanations: **A, C, D**. Answer **A** is incorrect because decrypting all protected volumes would make the disk readable in another system, but the data is no longer secured. Answer **C** is incorrect because it is not possible to remove a TPM module from a motherboard. Answer **D** is

incorrect because the checksum is secured on the TPM, not user accessible, and cannot be saved to a USB drive.

10. You are the administrator of a large enterprise network. The network contains domain-joined as well as nondomain-joined servers. You use WinRM for remote management. For nondomain servers you configured Basic authentication as the logon method. When you try to connect to a nondomain server, the connection is refused. What else do you have to configure to successfully connect?
 - A. Configure the nondomain server to use negotiation authentication.
 - B. On the nondomain server, request a certificate and configure WinRM to use the certificate for HTTPS.
 - C. On the client, request a certificate and configure WinRS to use the certificate for HTTPS.
 - D. Add an exception for the WinRM listener on the Windows firewall of the nondomain server.

Correct Answer and Explanation: **B.** Answer **B** is correct, because WinRM listeners accept only Basic or Digest authentication, when HTTPS is enabled by installing a certificate.

Incorrect Answers and Explanations: **A, C, D.** Answer **A** is incorrect because negotiation authentication works only on domain joined machines. Answer **C** is incorrect because adding a certificate would not help in establishing a secure channel with the server. A certificate must be installed on the server, not on the client. Answer **D** is incorrect because WinRM adds an exception to Windows firewall automatically when you configure WinRM for the first time.

Chapter 7: Developing a Public Key Infrastructure

1. You have been asked to provide an additional security system for your company's internet activity. This system should act as an underlying cryptography system. It should enable users or computers that have never been in trusted communication before to validate themselves by referencing an association to a trusted third party (TTP). The method of security the above example is referencing is?
 - A. Certificate Authority (CA)
 - B. Non-repudiation

- C. Cryptanalysis
- D. Public Key Infrastructure (PKI)

Correct Answer & Explanation: **D.** Answer **D** is correct because an underlying cryptography system that enables users or computers that have never been in trusted communication before to validate themselves by referencing an association to a trusted third party (TTP) is called a Public Key Infrastructure (PKI).

Incorrect Answers & Explanations: **A, B, C.** Answer **A** is incorrect, because Certificate Authority (CA) is a term that refers to the TTP in the PKI transaction. Answer **B** is incorrect, because it describes only one single goal of PKI. Answer **C** is incorrect; it refers to the process of decrypting or cracking data, not securing it.

2. You are engaged in an exercise that is meant to demonstrate the Public-Key Cryptography Standards (PKCS). You arrive at a portion of the exercise dealing with encrypting a string with a secret key based on a password. Which of the following PKCS does this exercise address?
 - A. PKCS #5
 - B. PKCS #1
 - C. PKCS #8
 - D. PKCS #9

Correct Answer & Explanation: **A.** PKCS #5 is correct because it is a Password-based Cryptography Standard that deals with the method for encrypting a string with a secret key that is derived from a password. The result of the method is an octet string (a sequence of 8-bit values).

Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because PKCS #1 deals with RSA Cryptography Standards and outlines the encryption of data using the RSA algorithm. The purpose of the RSA Cryptography Standard is in the development of digital signatures and digital envelopes. Answer **C** is incorrect, because PKCS #8 is the Private-key Information Syntax Standard and describes a method of communication for private-key information that includes the use of public-key algorithm and additional attributes (similar to PKCS #6). Answer **C** is incorrect, because PKCS #9 deals with Selected Attribute Types and defines the types of attributes for use in extended certificates (PKCS #6), digitally signed messages (PKCS #7), and private-key information (PKCS #8).

3. You are working in a Windows Server 2008 PKI and going over various user profiles that are subject to deletion due to company policy. The public keys for these users are stored under Documents and Settings\Administrator\System Certificates\My\Certificates and the private keys would be under Documents and Settings\Administrator\Crypto\RSA. You possess copies of the public keys in the registry, and in Active Directory. What effect will the deletion of the user profile have on the private key?
- A. It will have no effect.
 - B. It will be replaced by the public key that is stored.
 - C. The Private Key will be lost.
 - D. None of the above.

Correct Answer & Explanation: **C.** The private key will be lost if the user profile is deleted. The private keys are vulnerable to deletion and are stored under the user's profile.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, because the private keys are vulnerable to deletion and are stored under the user's profile, so deletion of the user profile will effect the private key. Answer **B** is incorrect, because the public key can not be used to replace the private key in any instance. Answer **D** is incorrect, because answer **C** is the correct answer.

4. Two users, Dave and Dixine, wish to communicate privately. Dave and Dixine each own a key pair consisting of a public key and a private key. If Dave wants Dixine to send him an encrypted message, which of the following security measures occurs first?
- A. Dave transmits his public key to Dixine.
 - B. Dixine uses Dave's public key to encrypt the message.
 - C. Nothing occurs the message is simply sent.
 - D. Dixine requests a access to Dave's private key.

Correct Answer & Explanation: **A.** Dave transmits his public key to Dixine is the correct answer because Dixine must receive Dave's public key to be able to encrypt the message so that Dave can use his private key to decrypt it.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because Dave must transmit his public key for Dixine to have access to it. This is the second step in the process not the first. Answer **C** is incorrect, because the

encryption process is not automatic and an exchange of public and private keys must occur for communication to be encrypted. Answer D is incorrect because private keys are never transmitted or shared and are used only to decode message encrypted with a matching public key pair.

5. You are browsing your company's e-commerce site using Internet Explorer 7 and have added a number of products to the shopping cart. You notice that there is a padlock symbol in the browser. By right clicking this symbol you will be able to view information concerning the site's:
 - A. Private Key.
 - B. Public Key.
 - C. Information Architecture.
 - D. Certificates.

Correct Answer & Explanation: C. Certificates is the correct answer because by clicking on the padlock you access the view Certificate information tab. This allows you to verify certain aspects of the certificate.

Incorrect Answers & Explanations: A, B, C. Answer A is incorrect, because you can never access another party's private key. Answer B is incorrect, because the public key has already been transmitted and is not accessible in this manner. Answer C is incorrect because information architecture (IA) of the site has nothing to do with the encryption process or PKI.

6. You are engaged in an exercise that is meant to demonstrate the Public-Key Cryptography Standards (PKCS) used in modern encryption. You arrive at a portion of the exercise which outlines the encryption of data using the RSA algorithm. Which of the following PKCS does this exercise address?
 - A. PKCS #5
 - B. PKCS #1
 - C. PKCS #8
 - D. PKCS #9

Correct Answer & Explanation: B. Answer B is correct, because PKCS #1 deals with RSA Cryptography Standards and outlines the encryption of data using the RSA algorithm. The purpose of the RSA Cryptography Standard is in the development of digital signatures and digital envelopes.

Incorrect Answers & Explanations: A, C, D. Answer A is incorrect; PKCS #5 is a Password-based Cryptography Standard that deals with the method for

encrypting a string with a secret key that is derived from a password. The result of the method is an octet string (a sequence of 8-bit values). Answer **C** is incorrect, because PKCS #8 is the Private-key Information Syntax Standard and describes a method of communication for private-key information that includes the use of public-key algorithm and additional attributes (similar to PKCS #6). Answer **D** is incorrect, because PKCS #9 deals with Selected Attribute Types and defines the types of attributes for use in extended certificates (PKCS #6), digitally signed messages (PKCS #7), and private-key information (PKCS #8).

7. You are the administrator of your company's Windows Server 2008 based network and are attempting to enroll a smart card and configure it at an enrollment station. Which of the following certificates must be requested in order to accomplish this action?
 - A. A machine certificate.
 - B. An application certificate.
 - C. A user certificate.
 - D. All of the above.

Correct Answer & Explanation: **C.** Answer **C** is correct because user certificates are certificates that enable the user to do something that would not be otherwise allowed. The Enrollment Agent certificate is one example of a user certificate. Without it, even an administrator is not able to enroll smart cards and configure them properly at an enrollment station.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, because machine certificates (as the name implies) give the system – instead of the user – the ability to do something out of the ordinary. The main purpose for machine certificates is authentication, both client-side and server-side. Answer **B** is incorrect, because the term application certificate refers to any certificate that is used with a specific PKI-enabled application. Examples include IPsec and S/MIME encryption for e-mail. Applications that need certificates are generally configured to automatically request them, and are then placed in a waiting status until the required certificate arrives. Answer **D** is incorrect because it is generally never required to for all of the listed certificates to be requested from a single action.

8. Dave and Dixine each own a key pair consisting of a public and private key. A public key was used to encrypt a message and the corresponding private key was used to decrypt. Dave wants Dixine to know that a document he

is responding with was really written by him. How is this possible using the given scenario?

- A. Dave's private key can encrypt the document and the matching public key can be used to decrypt it.
- B. Dave can send Dixine his private key as proof.
- C. Dixine can allow Dave access to her private key to encrypt the document.
- D. None of the above.

Correct Answer & Explanation: **A.** Dave's private key can be used to encrypt the document and the matching public key can be used to decrypt is the correct answer because if a user uses your public key to read the document and they are successful, they can be certain that it was "signed" by your private key and is therefore authentic.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** and **C** are incorrect, because private keys should never be shared with other users. Answer **D** is incorrect, as stated a private key can be used to encrypt a document so that the matching public key can be used to decrypt it.

9. You are administrating a large hierachal government environment in which a trust model needs to be established. The company does not want external CA involved in the verification process. Which of the following is the best trust model deployment for this scenario?
- A. A hierachal first party trust model.
 - B. A third-party single CA trust model.
 - C. A first-party single CA trust Model.
 - D. None of these will meet the needs of the company.

Correct Answer & Explanation: **A.** Choice **A** is correct because Hierarchical models work well in larger hierarchical environments, such as large government organizations or corporate environments and use multiple levels of subordinate CA that are governed by a root CA. First party CA are internal and administered by the company deploying them.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** and **C** are incorrect, because hierachal models are better suited for larger hierachal environments because they offer more layers of verification. Answer **D** is incorrect, because as stated choice A will meet the needs of this example.

10. Two users, Dave and Dixine, wish to communicate privately. Dave and Dixine each own a key pair consisting of a public key and a private key. A public key was used to encrypt a message and the corresponding private key was used to decrypt. What is the major security issue with this scenario?
- A. Private keys are revealed during the initial transaction.
 - B. Information encrypted with a public key can be decrypted too easily without the private key.
 - C. An attacker can intercept the data mid-stream, and replace the original signature with his or her own, using his private key.
 - D. None of the Above

Correct Answer & Explanation: **C.** Answer **C** is correct because there is nothing to prevent an attacker from intercepting the data mid-stream, and replacing the original signature with his or her own, using his private key. The solution to this problem in Windows PKI is the certificate.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, because private keys are never accessible to other users. Answer **B** is incorrect, because while the encryption process is not completely impervious to cracking without the private key to decrypt the data an attacker would have an incredibly hard time decrypting the transmission. Answer **D** is incorrect because as stated an attacker can intercept the data mid-stream, and replace the original signature with his or her own, using his private key.

Chapter 8: Planning for Server Virtualization

1. The hardware specific requirements for Windows Server Virtualization include processors with which feature included?
 - A. eXecute Disable memory access support
 - B. Data Execution Prevention
 - C. Virtual data execution protocol.
 - D. Monolithic hypervisor protocol support

Correct Answer & Explanation: **B.** Data Execution Prevention. This is a new security feature built in to Windows Server Virtualization designed to block hacker activity.

Incorrect Answers & Explanations: **A, C, D.** eXecute Disable technology (trade named “XD”) is the Intel trade name for their version of the hardware support for the eXecute Disable security feature. It does not have anything to do with the access of memory specifically, but rather the blocking of malicious code execution. Virtual data execution protocol and monolithic hypervisor protocol are non-existent terms.

2. Additional processor specific hardware functionality improvements for Windows Server Virtualization are required for which two reasons? (Choose two answers.)
 - A. Support for eXecute Disable memory access support
 - B. Support for additional security features
 - C. Enhanced performance characteristics for guest operating systems.
 - D. Assistance with hardware communication for guest operating systems

Correct Answers & Explanations: **B, D.** Support for additional security features refers to the Data Execution Prevention feature. Assistance with hardware communication for guest operating systems refers to the fact that Hyper-V uses hardware (processor) assistance to facilitate portions of communication between the guest operating systems and the underlying hardware. This is needed due to the fact that drivers are no longer contained within the hypervisor layer.

Incorrect Answers & Explanations: **A, C.** eXecute Disable technology (trade-named “XD”) is the Intel trade name for their version of the hardware support for the eXecute Disable security feature. It does not have anything to do with the access of memory specifically, but rather the blocking of malicious code execution. The hardware assistance required to support Hyper-Vs functionality is not associated directly with the performance characteristics of the guest operating systems.

3. Operating System Enlightenments apply to which partitions in Windows Server Virtualization architecture?
 - A. The parent partitions only
 - B. Both parent and child partitions
 - C. Child partitions only
 - D. The drivers running in the hypervisor layer

Correct Answer & Explanation: **C.** Operating system Enlightenments are the features within newer guest O/Ss that allow them to be aware of the fact that they are running on a virtual platform as opposed to physical hardware.

Incorrect Answers & Explanations: **A, B, D.** Operating system enlightenments do not affect the parent partition or the hypervisor layer. In effect they are the core components that make up the virtual platform and therefore there is no requirement to take extra measures to make them aware of the existence of said virtual platform.

4. Virtual Service Providers run in which part of the Windows Server Virtualization architecture?
 - A. In the Kernel Process layer of the parent partition.
 - B. In the User Process layer of the child partition.
 - C. In the User Process layer of the parent partition.
 - D. In the Kernel Process layer of the child partition.

Correct Answer & Explanation: **A.** Windows Server 2008 uses the Virtualization Service Providers (VSPs) to talk to the device drivers, and act as a proxy service to satisfy the hardware access requirements of the other guest operating systems running in the child partitions. This is a key part of what allows Windows Server 2008 Virtualization to work and it is a function that runs in the Kernel Process layer of the parent O/S. The VSPs form pairs with their corresponding Virtualization Service Clients running in the child partitions.

Incorrect Answers & Explanations: **B, C, D.** The VSPs run in the Kernel Processor layer of the parent O/S, and form pairs with their corresponding VSCs running in the child partitions. There are no VSPs running in the child partitions. Also VSPs are purely a Kernel Processor level within the parent partition, and do not run at the User Process level.

5. VM Worker Processes run in which part of the Windows Server Virtualization architecture?
 - A. In the Kernel Process layer of the parent partition.
 - B. In the User Process layer of the child partition.
 - C. In the User Process layer of the parent partition.
 - D. In the Kernel Process layer of the child partition.

Correct Answer & Explanation: **C.** The VM Worker Processes run within the virtualization stack, which in turn runs in the User Process level of the parent partition. Each VM has its own Virtual Machine Worker Process.

Incorrect Answers & Explanations: **A, B, D.** The VM Worker Processes run in the User Process layer and not Kernel layer of the parent O/S. VM Worker

Processes are designed to service the needs of the child partitions, but do not run within them.

6. VSP/VSC Pairs are used to accomplish what function in Windows Server Virtualization architecture?
 - A. They allow for memory to be reserved for exclusive use by the guest operating systems.
 - B. They allow the parent partition to communicate with child partitions which are running operating systems that have no enlightenments.
 - C. They allow the parent partition to support a longer list of legacy O/Ss.
 - D. They are used for communication of hardware access requests between the child and parent partitions across the VMBus.

Correct Answer & Explanation: **D.** The VSP/VSC Pairs provide the communication link for all resource requests from the child partitions. The VSP/VSC Pairs utilize the VMBus as their path of communication.

Incorrect Answers & Explanations: **A, B, C.** The VSP/VSC Pairs are not utilized by legacy guest O/Ss that possess no enlightenments, as enlightenments are a requirement for VSP/VSC communication. Legacy (non-enlightened) O/Ss use emulation to accomplish their hardware communication requirements. Guest O/Ss with enlightenments are a shorter list. In order to accomplish a longer list of supported guest O/Ss hardware emulation is the way to go.

7. Which of the following are prerequisites which must be in place to support an instance of Windows Server Virtualization? (Choose all that apply.)
 - A. Physical hardware running 64-bit processors
 - B. Physical hardware running processors which support Data Execution Prevention (DEP) technology
 - C. A minimum of 32Gb of memory
 - D. Windows Server 2008 Server Core installation

Correct Answer & Explanation: **B.** Support for Data Execution Prevention technology is a core requirement for underlying hardware to support an instance of Windows Server Virtualization.

Incorrect Answers & Explanations: **A, C, D.** It is not sufficient to run processors that are 64-bit to support Windows Server Virtualization. The processors must

have the specific functionality included to support the prerequisite features of Hyper-V. The HAL must be consulted to ensure compatibility prior to deployment. While a Windows Server Core installation is recommended, it is not a requirement. As well the minimum memory requirement of a Windows Server virtual platform is dependant upon the number of VMs to be deployed.

8. Which benefits can directly be associated with a move to virtualization in a data center? (Choose all that apply.)
 - A. Improved IT administrative efficiency
 - B. Reduced power consumption
 - C. Reduced cooling costs
 - D. Faster disk access times

Correct Answers & Explanations: **A, B, C.** Improved IT administrative efficiency, reduced power consumption, and reduced cooling costs are all direct benefits of a move to virtualization platforms, and the server consolidation that is made possible by this sort of migration.

Incorrect Answers & Explanations: **D.** Disk access times are not directly affected by a shift to virtualization, and in fact at the current level of technology development disk access times may actually be slightly reduced over what is possible with separate physical hardware platforms.

9. In a microkernel-style hypervisor model, in what partition component does the virtualization stack run?
 - A. In the Kernel Process layer of the parent partition.
 - B. In the User Process layer of the child partition.
 - C. There is no virtualization stack in a microkernel hypervisor.
 - D. In the parent partition.

Correct Answers & Explanations: **D.** The virtualization stack runs in the User Process level of the parent partition, and supports the VM Worker Processes. Each VM has its own Virtual Machine Worker Process.

Incorrect Answers & Explanations: **A, B, C.** The virtualization stack is Process a User level within the parent partition and, therefore, does not run in the Kernel Process layer. The microkernel hypervisor is the type of architecture used by Hyper-V, and therefore does contain a virtualization stack within its parent partition processes. The virtualization stack is designed to service the needs of the guest partitions, but does not run within them.

10. In a monolithic-style hypervisor model, what partition is used for Administrative Console access?
 - A. In the parent partition.
 - B. In one of the child partitions.
 - C. In one of the guest partitions.
 - D. The Administrative Console is not accessed through any of the partitions in monolithic hypervisor architecture.

Correct Answers & Explanations: **C.** The Administrative Console is accessed through one of the guest partitions in the monolithic-style hypervisor of architecture.

Incorrect Answers & Explanations: **A, B, D.** Parent and child partitions are components of the microkernel-style architecture. The monolithic hypervisor uses a different style of partition architecture.

Chapter 9: Planning for Business Continuity and High Availability

1. The Self Healing NTFS feature of Windows 2008 data storage can recover a volume under which of the following conditions? (Choose all that apply.)
 - A. The server cannot be started.
 - B. There is corrupt Data on the Volume.
 - C. The Volume is unreadable.
 - D. The Boot Sector is unreadable.

Correct Answers & Explanations: **B, C.** Self Healing NTFS has the ability to recover, or at least try to recover, individual files on a volume, as well as the entire volume should it become corrupted.

Incorrect Answers & Explanations: **A, D.** If the server cannot be started, then the volume could not be accessed whether it was corrupted or not. The server must at least be able to run in order to recover any of the data volumes hosted on it. As well, the Boot Sector must be readable, in order for Self Healing NTFS to be able to mount the volume for recovery.

2. What will occur in the event that Self Healing NTFS is unable to recover an individual file that has become corrupted?

- A. A message will be displayed on the screen, warning the user about what has happened.
- B. The file will be deleted.
- C. The file will be moved to a quarantine folder to allow for efforts to recover it.
- D. The file will be moved to the Recycle Bin where the user can choose to keep, or discard it.

Correct Answers & Explanations: **B.** In the event that a corrupted file cannot be recovered, it will be deleted. Since the file is already corrupted to the point where all efforts to recover it have failed, then at this point there is no benefit to keeping it anyway. It is essentially gone, and saving it will not make it any less gone.

Incorrect Answers & Explanations: **A, C, D.** A message will not be displayed on the screen warning the user about what has happened, but rather a warning will be generated in the event log. Since the file is already corrupted to the point where all efforts to recover it have failed, then at this point there is no benefit to keeping it by moving it to the Recycle Bin, or a Quarantine Folder for the purpose of allowing for further efforts to recover it. That's what backups are for.

- 3. Self Healing NTFS can be turned off by administrators who choose to do so. How will Self Healing NTFS behave when confronted with a corrupted file while its functionality is turned off?
 - A. It will still delete the file, but will not generate the event in the event log.
 - B. It will do nothing, as it is turned off, and therefore cannot function in any way.
 - C. It will generate the event in the event log, but take no action on the corrupted file.
 - D. It will try to recover the file, but then take no more action if unable to recover it.

Correct Answers & Explanations: **C.** When turned off, Self Healing NTFS will warn the user through the generation of an event in the event log, but will not take any action of any kind on the corrupted file in question. The user or administrator must manually take action to try to recover the corrupted file in this configuration.

Incorrect Answers & Explanations: **A, B, D.** When turned off, Self Healing NTFS will not take any action of any kind on the corrupted file in question. This includes deleting it, or trying to recover it. It is not however correct to say that it will not respond in any way, as it will still take the action to generate the warning event in the event log.

4. Multipath I/O is designed to support which of the following storage technologies? (Choose all that apply.)
 - A. iSCSI
 - B. Fiber
 - C. iSNS
 - D. SMB File Share

Correct Answers & Explanations: **A, B.** Multipath I/O is a technology that is designed to provide redundancy in the available paths between a server and its attached storage. The iSCSI protocol as well as Fiber based Host Bus Adapters (HBAs) are two of the most common methods of providing connectivity for attached storage. The iSCSI solution uses multiple NIC Cards to provide these redundant paths, and Fiber uses multiple HBAs, with attached fiber cable to provide redundant paths. Multipath I/O is simply the server side software designed to take advantage of these multiple paths when available.

Incorrect Answers & Explanations: **C, D.** iSNS is not used in conjunction with Multipath I/O, and SMB File Shares use the SMB protocol which communicates over the network through the onboard NICs. Multipath I/O only works with network connectivity when deployed in support of iSCSI.

5. When a storage controller is configured to use Multipath I/O in the Active / Active configuration the default configuration for Multipath I/O Load Balancing is which of the following?
 - A. Failback
 - B. Failover
 - C. Weighted Path
 - D. Round Robin

Correct Answers & Explanations: **B.** The default configuration for Multipath I/O Load Balancing when a storage controller is running in the Active / Active mode is Failover.

Incorrect Answers & Explanations: **A, C, D.** The Failback and Weighted Path are available options for selection during configuration, but are not the default selections. Round Robin is the default selection when the Storage Controller is of the Asymmetric Logical Unit Access type.

6. What would be the most effective way to prevent security violations and data theft in a Laboratory environment? (Choose all that apply).
 - A. Configure the BitLocker Drive Encryption Group Policy to encrypt all data stored on Laboratory server data volumes.
 - B. Deploy all Laboratory Servers of the Windows 2008 Server platform. Since BitLocker Drive Encryption is a built-in function with Windows 2008, it will protect all drives automatically by default.
 - C. Install the BitLocker Drive Encryption Role on all Laboratory Servers and configure it to encrypt all data stored on Laboratory server data volumes.
 - D. Configure the **Devices: Allowed to Format or Eject Removable Media** Group Policy to prohibit the use of removable media devices in the Lab environment.

Correct Answers & Explanations: **D.** The **Devices: Allowed to Format or Eject Removable Media** Group Policy is an effective method for the prevention of security violations and data theft in a Laboratory environment. This is especially true given that many laboratory environments are built on virtual platforms these days, meaning that entire servers are contained within one file that can easily be copied to removable media, and then transplanted on to any other like a virtual host, regardless of underlying hardware.

Incorrect Answers & Explanations: **A, B, C.** BitLocker Drive Encryption is not delivered in the form of a Group Policy, nor is it installed and enabled by default in Windows 2008 Server. In the case of answer **C**, while BitLocker Drive Encryption does need to be installed prior to being available for deployed, it is an optional feature, and not an actual Role.

7. By default, when installed and enabled, BitLocker Drive Encryption is designed to encrypt which of the following files? (Choose all that apply)
 - A. Paging files
 - B. Hibernation Files
 - C. All data on all volumes contained on the server

- D. Only the volumes that have been explicitly configured during installation to be covered by BitLocker Drive Encryption.

Correct Answers & Explanations: **A, B.** By default BitLocker Drive Encryption will provide encryption support for the System Volume, and all of the files contained within it. This would include any Paging and Hibernation files.

Incorrect Answers & Explanations: **C, D.** BitLocker Drive Encryption will not cover volumes beyond the system volume, unless explicitly configured to do so. It is not correct to say that it will only cover the volumes that have been explicitly configured during installation, since it does cover the system volume by default, without any configuration required.

8. BitLocker requires the assistance of TPM hardware support to provide complete protection for system files. It can however be configured to work on hardware that does not support the TPM standard. In this configuration, there will be some files that BitLocker Drive Encryption will not be able to protect. Which of the following will not be covered by BitLocker Driver Encryption when deployed and configured on non-TPM supported hardware? (Choose all that apply.)

- A. Paging Files
- B. The Master Boot Record
- C. The BIOS
- D. Hibernation files

Correct Answers & Explanations: **B, C.** When deployed and configured on non-TPM supported hardware, BitLocker Driver Encryption cannot provide support for the protection of pre-execution files used during initial startup. This includes files such as the BIOS and the Master Boot Record.

Incorrect Answers & Explanations: **A, D.** Files such as Paging and Hibernation will be covered when running on non-TPM supported hardware. Any files contained within volumes configured to be covered by BitLocker will be covered as long as the O/S is up and running. It is only the pre-execution files that cannot be protected without TPM hardware support.

9. In order to deploy a Microsoft Office Share Point Server 2007 solution on a Windows 2008 Server platform, which of the following prerequisites must be met? (Choose all that apply.)

- A. The Web Services optional server Role must be installed using Server Manager's **Add Features Wizard**.
- B. WSS 3.0 SP1 optional server feature must be installed.
- C. The Windows Process Activation Service must be installed.
- D. The .NET Framework 3.0 optional server feature must be installed using Server Manager's **Add Features Wizard**.

Correct Answers & Explanations: **C, D.** The Windows Process Activation Service and the .NET Framework 3.0 optional server feature are valid prerequisites for a deployment of Microsoft Office Share Point Server 2007. While WSS 3.0 SP1 is a valid prerequisite to the deployment of MOSS 2007, WSS 3.0 SP1 is a server Role, and not a feature.

Incorrect Answers & Explanations: **A, B.** The Web Services optional server Role cannot be installed using Server Manager's **Add Features Wizard**. Server Roles must be installed using the **Add Roles Wizard**. As well, WSS 3.0 SP1 is not a server feature, but rather a Role. It is also not installed using the standard method through Server Manager's **Add Role Wizard**. Instead Microsoft has chosen to deliver this server Role by means of an executable installation file.

10. Which of the following is the method used for the deployment of Windows Sharepoint Services 3.0 SP1 on a Windows 2008 Server platform?
 - A. The WSS 3.0 SP1 optional server Role must be installed using Server Manager's **Add Features Wizard**.
 - B. The WSS 3.0 SP1 optional server Role must be installed using Server Manager's **Add Roles Wizard**.
 - C. The WSS 3.0 SP1 optional server Role must be downloaded in the form of an executable file.
 - D. The WSS 3.0 SP1 optional server feature must be installed using Server Manager's **Add Features Wizard**.

Correct Answers & Explanations: **C.** The deployment of the **WSS 3.0 Server Role** is an exception to the normal Windows 2008 Server method of Role deployment where such items are simply selected under the **Add Roles Wizard** and installed on an as desired basis. According to Microsoft, it is their intent to maintain the deployment of the **WSS 3.0 Role** in this format for the foreseeable future.

Incorrect Answers & Explanations: **A, B, D**, As stated, the deployment of the **WSS 3.0 Server Role** is an exception to the normal Windows 2008 Server **Add Roles Wizard** method. This fact alone makes answer **B** incorrect. Answer **A** is incorrect because optional server Roles cannot be installed via the **Add Features Wizard**. Answer **D** is incorrect because WSS is a server Role, and not a feature.

Chapter 10: Software Updates and Compliance Management

1. You are the network administrator for a small company with ten Windows 2008 servers and 50 workstations in your domain. Currently, all of these machines are not being managed by any update policy and each may have individual settings that allow them to access the Internet to get updates. You would like to form a plan that will enable the workstations to receive updates with a minimum impact to the bandwidth footprint. What steps would you take to enable these machines?
 - A. Configure a local policy on each machine to force them to contact the Windows Update site every evening at midnight and apply all updates.
 - B. Create a Group Policy Object that would specify an update server and apply all approved policies.
 - C. Implement the Windows Server Update Services in your network and begin to approve updates on a regular basis.
 - D. Run the MBSA to determine what updates are missing on every machine.
 - E. Since this is a small environment, assign a network administrator the task of touching each machine once a week to ensure that patches are being applied.

Correct Answers: **B** and **C**. Implementing WSUS in your environment and requiring all machines to use this service on a regular basis through the GPOs available on the domain will require the least amount of administrative effort and will limit the bandwidth footprint by only downloading the patches once. This will also allow the network administrator to control the patches to be applied.

Incorrect Answers: **A, D**, and **E**. Configuring a local policy is difficult to maintain and still requires that each machine contacts the Windows Update site individually, causing the patches to be downloaded multiple times and

use excessive bandwidth. MBSA will uncover issues and provide a report of all required patches, but this is not an enabling technology. Doing the process manually requires significant manpower and can be expensive to maintain.

2. As the network administrator of a large corporate enterprise, it is your responsibility to ensure that all of the machines on your network are running the most current set of approved patches and updates. It is also important you are aware of any operating system security holes that have been introduced by some of your traveling power users who take their laptops with them as they go to client sites. What steps should you take to validate that workstations are in line with company policy?
 - A. Run the Microsoft Baseline Security Analyzer against the domain on a regular basis to poll the workstations.
 - B. Implement WSUS to push patches to the workstations.
 - C. Configure the lockdown settings outlined in the Windows Server 2008 Security Guide.
 - D. Require that every machine be attached to the domain to log on.
 - E. Turn on security auditing on the local machines.

Correct Answers: A. The MBSA is an auditing tool that is capable of comparing the system patch level against the Windows Update database, and which can validate a number of security settings on the operating system. This is a direct auditing tool and does not rely on the assumption that the configuration guarantees application of the policy. Additional steps such as enabling NAP and domain isolation would also help in a situation like this.

Incorrect Answers: B, C, D, and E. WSUS will certainly act as a resource through which machines can be brought into compliance with the required patch level, but this is not a direct auditing tool. The Security Best Practices are also important for controlling appropriate network access, but these settings are based on their deployment method and may not give a picture of the entire network. Finally, requiring that all machines be domain members or enabling security auditing will provide added control and tracking information, but cannot give you a complete centralized snapshot of your environment.

3. The company for which you are working started out as a very small organization where you were the only IT person, but the business is growing rapidly. You would like to protect access in your environment and enforce compliance with a single security standard for all server access. Because of the rapid growth,

you want to implement changes that are centrally managed, but you are still small enough to make structural changes without undue hardship to the business. What technologies should be at the core of your security compliance strategy?

- A. Implement the Windows Server Update Services.
- B. Create a domain security policy that enforces password complexity requirements.
- C. Implement the base OU and GPO structure provided in the GPO Accelerator Tool.
- D. Run the MBSA to determine what updates are missing on every machine.

Correct Answers: C. The GPO Accelerator Tool can provide both the Group Policy Objects and the base organization unit structure to implement the Windows Security Best Practices across multiple operating systems in your environment and to build a secure core of IT services. Using Active Directory and the Group Policy Management Console (GPMC), these changes can be centrally managed and deployed across your domain as it scales.

Incorrect Answers: A, B, and D. WSUS will not implement specific security best practices, though it is able to deploy security patches to machines in your environment. Enforcing secure passwords and a strong default domain policy is an important step in securing a domain, but this falls short of the objective. The full policy set deployed through the GPO Accelerator Tool is much more comprehensive and will bring the environment into compliance with best practices. Lastly, the MBSA is able to audit the environment for specific patch and security problems but does not have the ability to enforce policies or to act on specific problems.

- 4. You are working as the network administrator for a large enterprise with several large offices across the globe. Microsoft has released a major service pack for Windows Vista that is deployed to your workstation operating system at all locations. You should take several steps to validate that the patch is safe before rolling it out to all locations. What should be your first step in an appropriate rollout stratagem?
 - A. Deploy the service pack in a lab environment to ensure all mission-critical and line-of-business applications work as expected.
 - B. Deploy the service pack across the organization on a rolling schedule.
 - C. Deploy the service pack to a single site.

- D. Deploy the service pack to cross-functional test groups in each department of your organization.
- E. Deploy the service pack to test machines in a lab environment to test the OS.

Correct Answer: E. You should perform these steps in the following order:

1. Deploy the service pack to test machines in a lab environment to test the OS. This allows you to be sure there are no hardware problems that will affect your environment. This will also allow you to walk through deployment scenarios.
2. Deploy the service pack in a lab environment to ensure all mission-critical and line-of-business applications work as expected. In this step, you will be looking at the other application in your environment to be sure they will successfully run with the patch installed. With the large number of applications in the average enterprise, it will not be possible to test all of them, but for a major patch, the applications that will affect the ability of the business to function should be tested.
3. Deploy the service pack to cross-functional test groups in each department of your organization. Testing on friendly users across multiple departments should ensure these users will not be adversely affected by the patch and will also allow any applications not caught in the previous step, or that are very specialized, to be tested.
4. Deploy the service pack to a single site. Doing a test deployment on a smaller site or one that is not far from the network IT staff allows the impact of deployment problems to be minimized and problems to be addressed quickly.
5. Deploy the service pack across the organization on a rolling schedule. This is the larger corporate deployment where the full rollout plan is executed for the rest of the organization. This will generally be done on a rolling schedule to control potential risk and to allow appropriate staffing in case of problems.
5. The network that you administer has a number of different applications running. Your boss would like you to implement a patch management solution that will cover the majority of the Microsoft operating systems and programs in your environment. Which major applications will WSUS be able to update?
 - A. Configure a local policy on each machine to force them to contact the Windows Update site every evening at midnight and apply all updates.

- B. Create a Group Policy Object that would specify an update server and apply all approved policies.
- C. Implement the Windows Server Update Services in your network and begin to approve updates on a regular basis.
- D. Run the MBSA to determine what updates are missing on every machine.
- E. Since this is a small environment, assign a network administrator the task of touching each machine once a week to ensure patches are being applied.

Correct Answers: **B** and **C**. Implementing WSUS in your environment and requiring all machines to use this service on a regular basis through the GPOs available on the domain will require the least amount of administrative effort and will limit the bandwidth footprint by only downloading the patches once. This will also allow the network administrator to control the patches to be applied.

Incorrect Answers: **A**, **D**, and **E**. Configuring a local policy is difficult to maintain and still requires that each machine contacts the Windows Update site individually, causing the patches to be downloaded multiple times and use excessive bandwidth. MBSA will uncover issues and provide a report of all required patches, but this is not an enabling technology. Doing the process manually requires significant manpower and can be expensive to maintain.

- 6. The director of IT would like you to deploy a patch management solution that will be capable of ensuring all workstations and servers in your network are able to get operating system patches that have been internally tested. You are planning to deploy WSUS to meet this need. Unfortunately, you have a number of legacy machines in your environment. You will need to upgrade a number of workstations before they will be able to participate in WSUS updates. Which machines will you have to replace or upgrade?
 - A. Windows Server 2000 SP2
 - B. Windows ME
 - C. Windows XP SP2
 - D. Windows 2000 Workstation SP4
 - E. Windows NT Server

Correct Answers: **A**, **B**, and **E**. Windows ME and Windows NT 4.0 are not compatible with WSUS to receive updates. Windows Server 2000 can receive updates from WSUS, but it must first be updated to Service Pack 4 first.

Incorrect Answers: C and D. Both of these can participate in WSUS updates. Remember that WSUS only supports Windows Server 2008, Windows 2003, Windows Vista, Windows XP SP2 and later, and Windows 2000 SP4 for updates. In order to run the WSUS service for the domain, the server must be Windows Server 2008 or 2003 SP1.

7. Your network has been built using a highly decentralized model with a central headquarters and large independent branch offices, each with their own IT departments and standards. You would like to implement WSUS in your environment but need to ensure that each branch office has control over the patches deployed in their branch offices. How should you configure WSUS to ensure these requirements are met?
 - A. Implement WSUS as an enterprise service and allow the branch offices to manage their own group policies to control whether or not the machines on their local segments will attach to the central WSUS servers.
 - B. Implement a centrally configured WSUS server and additional WSUS servers at each branch office that will receive their patches from the central site, but be able to control the patch approval and deployment at each site.
 - C. Configure WSUS at the central site but still allow the individual branch offices to go directly to the Microsoft Update site to get their patches.
 - D. Implement WSUS independently at each of the branch offices with separate site GPOs controlling WSUS membership.

Correct Answers: D. While there is some overhead in downloading the patch catalog and updates at each site, this is the only way to ensure that decisions made at the central site will not impact the individual offices or their workstations.

Incorrect Answers: A, B, and C. None of these options meet the requirements of both autonomy and enterprise management. Simply allowing the branch offices to avoid deploying the GPO that will bind them to the central server will leave you open to vulnerabilities that would be associated with not having patched machines on your networked machines. In many circumstances, having a hierarchical structure is highly desirable. Since these subordinate servers will receive their patches from the central server, decisions made here will have some impact on these other servers. In environments where complete isolation is needed, you cannot rely on this structure to provide the needed flexibility. Finally, allowing the workstations to go directly to the

Microsoft Update site will remove the network administrators' ability to centrally manage the workstations, even at the site level. Some configuration of WSUS is thus required to manage these machines appropriately.

8. You are the network administrator of a large enterprise planning to deploy WSUS servers as a centralized patch management platform. You would like to ensure this service is implemented in a highly available manner. You want to be sure you are providing an adequate database structure to support this environment. What database configuration should you choose to provide the appropriate availability for your implementation?
 - A. Allow the WSUS servers to use their internal database to manage the datastore.
 - B. Implement a cluster of SQL 2005 databases to house the datastore.
 - C. Store the database on a server running SQL 2005.
 - D. Configure Microsoft Access 2007 to house the datastore.
 - E. Use the SQL 2000 Cluster you already have in your environment to house the databases.

Correct Answers: **B.** In order to provide the maximum availability to the WSUS servers, a cluster of SQL 2005 SP2 servers can be used to ensure that the needed data resources are always present. This will allow the failure of an individual server or data resource to have only a minimal impact on the WSUS implementation since the secondary server will be able to assume the load.

Incorrect Answers: **A, C, D, and E.** In order to provide a high-availability implementation, a cluster of SQL servers is required. Neither the internal database nor a standalone implementation of SQL will provide redundancy in the event of database or hardware failure. In order for WSUS to function, the database must be Microsoft SQL 2005 Sp1 or later. Neither Access 2007 nor a cluster of SQL 2000 servers are able to run the WSUS databases.

9. You are planning a testing lab environment so you can evaluate the impact of patches on your business before releasing them for wide deployment. You would like to keep the environment as small as possible so your costs are controlled, but you also need to ensure that patch deployment will not cripple your business. What resources should you implement in your patch testing lab?
 - A. You must represent every application you have deployed in the wild in your lab environment.

- B. You should duplicate all servers in your server environment to be sure there will be no conflicts.
- C. You should have a representative of each major workstation base image in your test environment.
- D. You should have an environment capable of running each of the mission-critical applications on your network.

Correct Answers: C and D. You should ensure there are no major compatibility issues with your mission-critical applications or with the workstation images you have deployed in your environment. This will help ensure that deployed updates will not have a negative update on your environment to the point where you are no longer able to function.

Incorrect Answers: A and B. In a perfect world, you would be able to provide 100% coverage of applications and servers in your environment. This is usually not possible because of the large number of applications deployed across the average business and the expense of maintaining a duplicate testing environment. This is further complicated by the frequency at which updates are deployed. In short, it is nearly impossible to manage patch management to this level of surety. This risk can be greatly mitigated through the judicious testing of important applications as well as controlled User Acceptance Testing before a patch is rolled out for full enterprise deployment.

- 10. You are planning to delegate the management of WSUS patches to lower level systems administrators on your network. You are concerned that the deployment of some kinds of patches might pose a larger risk to your environment without thorough testing and high-level approval. To address this, you are planning a two-level WSUS deployment where your systems administrators will only be able to deploy certain types of patches, but you will still be able to receive the full patch set centrally. Which classifications should you exclude from the lower level deployment?
 - A. Drivers
 - B. Service Packs
 - C. Critical Updates
 - D. Definition Updates
 - E. Update Rollups

Correct Answers: A and B. Drivers and service packs both have the potential to cause server impacts on the workstations in your environment. Drivers can

affect the Windows Operation System's ability to communicate with the hardware and should be tested thoroughly before being rolled out. Service packs contain major functionality changes to the operating systems and should also be thoroughly tested.

Incorrect Answers: **C**, **D**, and **E**. All of these patch types are part of the normal maintenance of the Windows operating system and the security landscape. Application of these kinds of updates directly contributes to the security of the workstations and has been released to specifically address known vulnerabilities in the operating system.

Index

A

- AAAA address, 16
Access control lists
 description of, 104, 215, 240
 security, 247–248
 system, 247–248, 252
Accounts
 cached, 469
 computer
 migration of, 346–348
 read-only domain controller, 457–460
ACLs. *See* Access control lists
Active Directory
 BitLocker information stored in, 439–445
 components of, 249
 DNS server installation with, 27–29
 domain controllers, 204
 forest. *See* Forest
 groups, 241–245, 252
 GUID in, 331
 preparation of, for Windows Server 2008
 domain controllers installation, 350–351
 replication, 412–413
 schema
 extending of, for BitLocker backup
 information, 442–444
 modifications, 218–220
 stability risks, 587
 Unix system attributes configured for, 387–388
Active Directory Administrative Model
 access lists, 241
 compliance auditing, 245–247
 delegation, 240–241
 description of, 239–240
 global audit policy, 247
group strategy, 241–245
SACLs, 247–248, 252
schema, 248
Active Directory Application Mode, 377–378
Active Directory domain
 description of, 201–202
 upgrading of, 348–351
Active Directory Domain Services
 description of, 186
 fine-grained password policies, 187–190
 installing of, using Windows Interface, 206–208
 logical structure
 description of, 199–200
 organizational units, 202–203
 trees, 200–201
 multi-master replication of directory
 data supported by, 220
 physical design structure, 204–205
 read-only, 191
 skipping of, during domain controller
 installation, 456
 subnets, 205
 User Interface, 192
Active Directory Federation Services
 configuring, 364–376
 description of, 329, 361–362, 396
 prerequisites for, 364
Active Directory Lightweight Directory Services. *See* AD LDS
Active Directory Migration Tool
 description of, 333
 domain restructuring using, 334
 installing, 335
 password export server, 337–338
Active Directory Objects, 296–306
Active Directory Service Interfaces. *See* ADSI

- Active Directory Sites and Services snap-in, 382
- Active Directory topology
 - description of, 220–221
 - forest root domain controllers, 222
 - global catalog servers, 226, 228–231
 - infrastructure master, 225–226
 - location policies, 235–238
 - networks with limited connectivity, 226–228
 - operations master, 224–225, 251
 - PDC emulator, 225
 - printer policies, 235–238
 - regional domain controllers, 222–224
 - server placement, 222–235
 - site link bridge, 233–234
 - site link objects, 231–233
 - site objects, 231–233
 - subnet objects, 235
- Active Directory tree, 200–201
- Active Directory–integrated zones
 - description of, 18, 21–22
 - questions regarding, 74
 - Secure dynamic updates, 32
- AD LDS
 - Administrators Page, 381
 - configuring, 378–381
 - description of, 376–377, 396
 - multiple instances of, 399
 - replication of information, 400
 - when to use, 377
 - working with, 381–382
- ADAM, 377–378
- ADDS, 400
- Administration Server (NAP), 95
- Administrative Template files, 265, 286–287
- ADM files, 265–268, 286–287
- ADMT. *See* Active Directory Migration Tool
- ADMX files, 265–268
- ADSI, 381
- ADS&S snap-in, 382
- Advanced Encryption Standard, 216–217
- .aero, 5
- Aging policies, for DNS server, 35–38
- Application certificates, 526
- Application patching, 774
- Application Virtualization, 640
- AS-REQ/REP, 216
- Attributes, 218
- Auditing, 82–83, 245–247
- Auditor, 542
- Authentication
 - BitLocker modes, 424–426
 - centralized account administration, 409
 - description of, 82–83
 - intra-organizational, 215–217
 - Kerberos, 410
 - password policies, 410–411
 - PIN, 425, 427
 - public key cryptography for, 511–512
 - Public Key Infrastructure, 494–495
 - single sign-on applications, 409–410
- Authentication Protocols
 - challenge-handshake, 151
 - extensible, 151–152
 - password, 151
 - virtual private network, 150–152
- Authoritative answer, 14
- Authoritative DNS server, 70
- Authoritative Restore of Directory Services, 721, 723
- Authorization
 - description of, 82–83
 - intra-organizational, 215–217

B

- Background Intelligent Transfer service, 750
- Background refresh interval, 275–276, 318
- Backup
 - description of, 407
 - Directory Services, 719–720

- dynamic, 660
- Full Server Backup, 706–715
 - planning for, 701–715
 - Server, 701–715, 723–730
 - virtualization benefits for, 716
- Backup Operator, 542
- Backward compatibility, 330
- Bare Metal Restore, 717–719
- Baseline
 - definition of, 775
 - description of, 745, 774–775
- Baseline Security Analyzer
 - analyzing results, 786–787
 - archiving baselines using, 795
 - configuring, 784–786
 - description of, 783
 - Microsoft Update and, comparisons
 - between, 783–784
 - summary of, 793
- BIOS, 592
- BitLocker
 - Active Directory storage of information, 439–445
 - administration of, 437
 - architecture of, 422–423
 - authentication modes, 424–426
 - data recovery procedures, 445–447
 - for data volumes, 434
 - disabling, 447
 - Drive Encryption, 668–671
 - enabling, 427–429
 - encryption, 419, 421, 423–424, 484
 - Extensible Firmware Interface
 - computers, 426
 - full volume encryption, 419, 423–424
 - Group Policy with
 - description of, 437–439
 - settings for, 422, 424, 444–445
 - hardware upgrades on systems
 - protected with, 424
- installing, 426, 429–430
- Management Options, 670–671
- multifactor authentication, 426–427
- on Windows Vista, 428
- overview of, 418
- partitioning disks for, 427–429
- password saving, 432
- PIN authentication modes, 425, 427
- recovery
 - mechanisms, 420
 - procedures for, 445–447
 - storage of information in Active Directory, 439–445
- remote administration, 421
- requirements for, 417
- safe decommission of hardware
 - using, 671
- secure decommissioning, 421
- software requirements for, 417
- startup key authentication, 427
- startup process integrity verification, 419–420
- summary of, 480–481
- for TPM-less operation, 434–437
- Trusted Platform Modules, 417–418, 669
- turning off, 447
- turning on, 431–434
- volume encryption, 419, 421, 423–424, 484
- Volume Recovery, 670
- when to use, 426–427
- Windows Management Instrumentation interface, 437
- Windows Server 2008 installation, 429–430
- BitLocker Drive Security, 736
- Bitmap caching, 143–144
- .biz, 5
- Block Inheritance, 307–308
- b-node, 48

- Branch offices
 - backup and restore concerns, 407
 - challenges associated with, 406–409
 - domain controller in, 411–414
 - hub-and-spoke topology for, 408–409
 - network bandwidth for, 406
 - security issues, 406–407
 - user population, 411–412
- Windows Server Update Services
 - deployment, 755–756
- Bulk data encryption, 512–524
- Burst handling, 60–62
- Business to Business solutions, 328, 360
- Business to Customer solutions, 328, 360

- C**
- Caching
 - credential, 449–450, 468–469
 - NetBIOS, 52
 - Universal group membership, 415–416, 484
- Central store, 267
- Centralized account administration, 409
- Certificate(s)
 - application, 526
 - expiration of, 544
 - machine, 526
 - organization's need for, 526–527
 - purpose of, 528
 - revocation of, 543–547, 573
 - user, 525, 573
 - validity period, 573–574
 - versioning, 566–567
- Certificate authority
 - configuring, 527–535
 - creation of, 530, 569–570
 - definition of, 496, 507, 527–528
 - description of, 493
 - enterprise, 528–529, 570
 - hierarchy, 573
 - installation considerations, 533
- intermediate, 530
- internal, 527
- revocation of certificates by, 543–547
- root, 529–530, 562, 573
- standard, 528–529
- subordinate, 529–530, 562
- summary of, 569–570
- X.509 standard used by, 506–507, 545, 572
- Certificate Authority administrator, 542
- Certificate enrollment, 532
- Certificate manager, 542
- Certificate practice statement, 535
- Certificate requests, 530–534
- Certificate revocation lists, 545, 573
- Certificate Rule, 281
- Certificate Services
 - backing up, 535–538
 - installing, 514–523
 - mechanism of operation, 513
 - restoring, 538–541
 - working with, 527
- Certificate templates
 - Computer, 560–562
 - Cross-Certification Authority, 562
 - Cryptography, 552–553
 - custom, 562–565
 - description of, 547
 - Directory E-mail Replication, 562
 - Domain Controller, 562
 - Extensions, 556–557
 - General Properties, 549–550
 - Issuance Requirements, 555–556
 - permissions, 565–566
 - Request Handling, 551–552
 - Security, 557–559
 - snap-in, 548
 - Subject Name, 554
 - types of, 559–565
 - User, 559–560
 - versioning, 566–567

Challenge-handshake authentication protocol, 151
 Checksum, 67
 Child domains, 6, 20
 Child partitions, 595
 Citrix Systems, 106, 113
 Class, 218
 Client Access Licenses, 107, 122, 134–135
 Cloning, 355, 395
 Cluster Continuous Replication, 696
 CNAME, 16
 .com, 5
 Compliance, 746–747
 Compliance auditing, 245–247
 Computer accounts
 migration of, 346–348
 read-only domain controller, 457–460
 Computer Certificate Templates, 560–562
 Computer names, 39
 Condition forwarding, 23
 .coop, 5
 Corporate desktop, 116–117
 Credential caching, 449–450, 468–469
 Critical updates, 751
 Cross-Certification Authority
 certificate, 562
 Cross-forest authentication, 359–360
 Cross-platform interoperability
 description of, 383
 file system paths, 383–384
 Unix systems. *See* Unix systems
 Cryptography
 certificate templates, 552–553
 definition of, 495
 history of, 498–499
 public-key, 500–505
 shared secret key, 500
 Cryptography Next Generation, 498
 Custom certificate templates, 562–565

D

Data collaboration, 672–673
 Data encryption standard, 499
 Data execution prevention, 592
 Data management
 definition of, 664
 Share and Storage Management
 Console, 664–665
 Storage Explorer Console, 665–666
 Storage Manager for SANs Console, 666–667
 Data recovery
 BitLocker, 445–447
 strategies for, 716–717
 Data redundancy
 description of, 660
 Distributed File System for, 699–700
 Data security
 description of, 667
 Group Policy Control over removable media, 667–668
 Data transfer, 149
 Database Mounting Tool, 191
 Database scavenging, 55
 Definition updates, 751
 Demilitarized domain, 363
 Demilitarized zones
 definition of, 377
 networks, 161
 purpose of, 377
 Denial of service, 149, 774–775
 DES, 499
 Device installation
 by computer, 312–314
 Group Policy used to control, 312–314
 by user, 314
 DFS. *See* Distributed File System
 DFS-R, 407

- DHCP
 configuring of, for NAP, 97–103
 description of, 697
 server, 11, 31
- Differentiated Services Code Point value, 291
- Diffie-Hellman Key Agreement, 501
- Digital signatures
 creation of, 504, 511, 569, 572
 definition of, 510
 mechanism of operation, 506–509
 purpose of, 510
- Directory E-mail Replication
 certificate, 562
- Directory enabled applications, 358
- Directory Services
 Authoritative Restore, 721, 723
 backup, 719–720, 738
 Non-Authoritative Restore, 721–722
 recovering, 719–723
 Restore Mode Recovery, 720–721
- Disaster recovery, 587–588, 660–661
- Disconnection, 139
- Distributed File System
 data redundancy uses, 699–700
 Namespace Service, 700
 Redundancy, 697
 Replication, 407
 Replication Service, 700
- Distributed Transaction Coordinator, 697
- Distribution group, 242
- DMZs. *See* Demilitarized zones
- DNS
 client settings, 38–39
 client/server protocol, 6–7
 definition of, 5, 68
 description of, 3
 dynamic updates, 32
 host names, 5
 local resolver, 3
 need for, 8
- NetBIOS vs., 4
 resolver cache, 11, 43–44
 resource records, 15–17
 separate name design of, 26–27
 split-brain design of, 24–26
 suffixes, 40–42
 Windows Server 2008
 enhancements, 7–8
- DNS query
 creation of, 9
 forward lookup, 9
 message elements, 10
 process involved in, 10–14
 responses to, 14–15
 reverse lookup, 9–10
 summary of, 70
- DNS server
 with Active Directory, 27–29
 aging policies, 35–38
 authoritative, 70
 computer names, 39
 configuring, 68
 installation and implementation of
 separate name design, 26
 Server Manager for, 30
 split-brain design, 25
 summary of, 71
 querying, 11–14, 44
 scavenging policies, 35–38
 static IP addresses on, 31
 WINS server integration with, 44–45
- DNS zones
 Active Directory–integrated zones, 18, 21–22
 condition forwarding, 23
 configuration of, 20–21
 creation of, 33–35
 definition of, 70
 Forward lookup zones, 33
 GlobalNames, 8, 19, 23–24
 implementation of, 19–20

non Active Directory–integrated zones, 19–20
on read-only domain controllers, 452
Reverse lookup zones, 34
secondary, 18, 23
selection of, 35
stub, 18, 23
types of, 17–19
WINS integration in, 45
Document folders, redirecting of, 282–284
Domain controllers
autoenrollment, 574
certificate, 562
description of, 204
forest root, 222
full, 416–417
global catalog servers, 226
installing of, in existing forest, 350–351
password storage, 448
PDC. *See* PDC emulator
physical security, 412
processing of Group Policy Objects, 270–272
read-only. *See* Read-only domain controller
regional, 222–224
in remote office, 411–414, 484
Domain functional levels, 209–213, 350
Domain Group Policy, 769
Domain Isolation
benefits of, 171
overview of, 169–170
schematic diagram of, 172
strategy for, 172–174
Domain name system. *See* DNS
Domain names
child, 6, 20
examples of, 5

forest, 194
fully qualified, 6–7, 23, 42–43
naming system for, 5
parent, 6, 20
Domain-based distributed file system, 199
Domain-Naming Master, 221
Drivers, 751–752
Dynamic backup, 660
Dynamic host configuration protocol server. *See* DHCP, server

E

.edu, 5
Emergency Management Service, 475
Encrypting File System, 419, 559, 572
Encryption
bulk data, 512–524
full volume, 419, 421, 423–424, 484
hash function, 499
history of, 498–499
public key, 499–500
secret key, 499, 512
session key, 512
symmetric key, 499
Enforcement Clients. *See* NAP, Enforcement Clients
Enforcement Server (NAP), 95–96
Enterprise certificate authority, 528–529, 570
Enterprise Client Environment, 777, 792
Enterprise health management plan, 745
Enterprise Public Key Infrastructure, 497
Enterprise Trust, 281
ESX Server, 626–627
Extended certificates, 501
Extensible authentication protocol, 151–152
External names, 4, 74
External Trusts, 359

F

Failover clustering
 description of, 677
 file services cluster, 698–699
 heartbeat–configurable delay, 695
 Hyper-V, 700
 installing, 680–694
 Management Console, 694
 multi-site clusters, 694–695
 prerequisites for, 698
 service availability, 697
 Service Redundancy, 695–696
 subnet flexibility, 695
 Windows 2008 improvements in, 677–679

Feature packs, 752

Federation
 definition of, 362
 uses of, 362–363

File services cluster, 698–699

File transfer protocol, 291

Fine-grained password policies, 187–190, 410

Firewall
 description of, 164
 Windows Firewall with Advanced Security, 166–169, 179

Flexible Single Master Operations, 271

Folder redirection settings, 282–284

Forest
 Active Directory Domain Services
 logical design structure, 199–200
 cross-forest authentication, 359–360
 definition of, 200
 domains in, 200
 function levels, 209–213
 new, 215
 number of, 105
 purpose of, 251
 read-only domain controller
 added to, 453

upgrading, 213–215
 upgrading of, 348–351
 Windows Server 2008 domain controllers
 installed into, 350–351

Forest design
 administrative overhead considerations, 195–196
 business units and, 193–194
 factors to consider in, 193–196
 namespaces, 194
 plan for, 196–198
 steps involved in, 197–198
 testing environments, 196
 timelines for, 195

Forest Discovery Scope, 132

Forest root domain, 206, 399

Forest root domain controllers, 222

Forest Trusts, 356, 359

Forward lookup queries, 9

Forward lookup zones, 33

FQDN. *See* Fully qualified domain name

Full domain controllers, 416–417

Fully qualified domain name, 6–7, 24, 42–43

G

Genetic Routing Encapsulation, 152

Geographically disbursed clustering, 738

Global audit policy, 247

Global catalog servers
 description of, 226, 228–231
 placement of, 414–415
 in remote office, 414–415

Global groups, 243

Global Unique Identifier. *See* GUID

Globally Unique Identifier, 313

GlobalNames zone, 8, 19, 23–24, 195

.gov, 6

Group Policy
 Administrative Templates, 286–287, 294
 background refresh interval, 275–276, 318

- BitLocker with
 - description of, 437–439
 - settings, 422, 424, 444–445
- computer policies, 287–288
 - controlling device installation by computer, 312–314
 - description of, 312
 - by user, 314
 - folder redirection settings, 282–284
 - hierarchies, 307–308
 - logoff scripts, 284–285
 - logon scripts, 284–285, 318
 - processing of
 - on read-only domain controllers, 485
 - over remote access connections, 275
 - over slow links, 273–275
 - refresh interval, 275–276
 - remote administration, 479
 - Restricted Groups, 289–290
 - RSoP, 300–303
 - security settings, 281–282
 - shutdown scripts, 293–294
 - software installation, 280–281, 288–289, 318
 - startup scripts, 293–294
 - Windows PowerShell used to manage, 303–306
- Group Policy Control over removable media, 667–668
- Group Policy Management Console, 160, 266, 269, 277, 776
- Group Policy Object Accelerator Tool
 - configuring, 778–783
 - description of, 775–776
 - requirements, 777
 - security baselines supported by, 777–778
 - security policies implemented using, 796
 - summary of, 791–792
- Group Policy Objects
 - backing up, 276–279
 - conflicts, 297–300
- Corporate Desktop, 299
 - default permissions, 309
 - description of, 195, 202, 262
 - domain controller that process, 270–272
 - filtering, 769
 - linking of
 - to Active Directory Objects, 296–306
 - description of, 296–297
 - to organizational units, 297, 306
 - organizational units linked to, 269
- Preferences
 - ADMX/ADML files, 265–268
 - description of, 479
 - location of, 263
 - mapping a network drive in, 264–265
 - overview of, 262–263
- processing of
 - order of, 298
 - over remote access connections, 275
 - over slow links, 273–275
- restoring, 276–279
- Standard Desktop, 299
- Starter, 295–296
- templates, 295
- user policies, 279
- uses of, 268
- Groups
 - description of, 241–245, 252
 - migration of, 339–342
- GSSAPI, 216
- GSS-SPNEGO, 216
- Guest operating systems, 595–596
- GUID
 - description of, 331
 - domain object, 332
 - restructuring effect on, 332–333

H

- Hackers, 589
- Hardware redundancy, 660
- Hash function, 499

- Hash Rule, 282
- HCAP.** *See Host Credential Authorization Protocol*
- Health modeling, 745
- Health Policy Server (NAP), 95
- Health Registration Authority (NAP), 95
- High availability
- data accessibility and redundancy, 697
 - definition of, 677
 - failover clustering. *See Failover clustering*
 - virtualization and, 700–701
- h-node, 48, 75
- Host Credential Authorization Protocol**, 97
- Host names, 5
- HOSTS file, 46–47, 71
- HTTP, 361
- Hub-and-spoke topology, 408–409
- Hyper-V**
- description of, 600–601
 - Failover Clustering, 700
 - high availability with, 700–701
 - Manager Console, 616–624
 - RCO update, 601–614
 - Server Core installation, 624–626
 - virtual machines configured with, 614–624
- Hypervisor**
- microkernel, 590–591
 - monolithic, 588–590
- I**
- IIS 6.0 Management Compatibility Component, 673
- .info, 6
- Infrastructure master, 225–226
- .int, 6
- Inter-forest restructuring, 330, 355, 357–358, 395
- Intermediate certificate authority, 530
- Internal names, 4, 74
- Internet Authorization Service, 178
- Interoperability
- Active Directory Federation Services, 361–362
 - Application Authorization, 376–377
 - cross-platform. *See Cross-platform interoperability*
 - interorganizational strategies, 361
 - planning for, 360–361
- Intersite replication, 412
- Intra-forest restructuring, 330, 353–357, 395
- Intrasite replication, 412
- IP addresses
- HOSTS file, 46–47
 - static
 - assignment message for, 31
 - on DNS server, 31
 - Ipconfig/displaydns, 44
 - Ipconfig/flushdns, 44
 - Ipconfig/registerdns, 44
 - IPsec, 561
 - IPv4, 66–67
 - IPv6
 - address pool, 66
 - features of, 66–67, 73
 - IPv4 vs., 66–67
 - jumbograms, 67
 - network-layer security, 67
 - stateless address auto configuration, 66
 - Windows Server 2008 support for, 7
- ISP, 105
- J**
- Jumbograms, 67
- K**
- Kerberos, 215, 410
- Kerberos ticket account, 450–451
- Key Distribution Center
- description of, 215
 - Kerberos, 410

Key pairs, 494, 496
 Key recovery, 535
 Key recovery agent, 567–568

L

Legacy guest operating system, 596
 Link-local multicast name resolution.
See LLMR
 LLMR, 8
 LMHOSTS file, 3, 50, 63–65, 73
 Local Group Policy, 769
 Local network access, 84
 Local resolver, 3, 10–11
 Location policies, 235–238
 Logoff scripts, 284–285
 Logon scripts, 284–285, 318, 411
 L2TP/IPSec, 153–154

M

Machine certificates, 526
 Majority Quorum Model, 679
 Malware, 148
 Man-in-the-middle attack, 149
 Media Transfer Protocol, 142
 Memory curtaining, 418
 Memory keys, 668
 Microkernel hypervisor, 590–591
 Microsoft Baseline Security Analyzer
analyzing results, 786–787
archiving baselines using, 795
configuring, 784–786
description of, 783
Microsoft Update and, comparisons between, 783–784
summary of, 793
 Microsoft Challenge Handshake Authentication Protocol, 151
 Microsoft Exchange Server, 409, 485
 Microsoft Office Communication Server, 362
 Microsoft Server virtualization, 597–601

Microsoft Solutions Framework, 352, 395
 Microsoft Update
 Microsoft Baseline Security Analyzer and, comparisons between, 783–784
 patch management, 753–754

Migration

backward compatibility issues, 330
 computer accounts, 346–348
 groups, 339–342
 indications for, 329–330
 inter-forest, 330, 355, 357–358
 intra-forest, 330, 353–357
 object, 330–348, 395
 planning of, 352–353
 System Center Virtual Machine Manager 2007 support, 636–637, 653
 user accounts, 339, 343–345

.mil, 6

m-node, 48
 Modulo algebra, 505
 Monolithic hypervisor, 588–590
 Multicasting, 58, 66–67
 Multipath I/O, 663–664
 Multi-site clustering, 694–695
 .museum, 6
 MX, 16

N

Name(s)
domain. See Domain names
external, 4
host, 5
internal, 4
NetBIOS, 40–43, 47–48, 69, 74–75
public, 4
WINS server registration, 51–52
.name, 6
 Name resolution
DNS method. See DNS
NetBIOS method, 3–4
overview of, 2–3

- Name server records, 16, 23
- Naming strategy, 2–3
- NAP
 - adding, 90–91
 - Administration Server, 95
 - Agent, 93
 - benefits of, 103
 - client components, 92–94
 - communication schematic for, 92
 - DHCP configured for, 97–103
 - Enforcement Clients, 93–94
 - Enforcement Point, 95–96
 - Enforcement Server, 95–96
 - Health Policy Server, 95
 - Health Registration Authority, 95
 - Health Service Validator, 789
 - network design for, 103–104
 - networking services, 97
 - purpose of, 89
 - questions regarding, 178
 - Remediation Server, 96
 - Requirement Server, 96
 - servers that support, 91
 - Statement of Health Response, 93, 97
 - System Health Agent, 92–93
 - System Health Validators, 95
- NBT. *See* NetBIOS, over TCP/IP
- Negative answer, 15
- .net, 6
- .NET environment, 673–674
- NetBIOS
 - cache, 52, 75
 - DNS vs., 3–4
 - LMHOSTS file, 3, 50, 63–65, 73
 - names, 40–43, 47–48, 69, 74–75
 - node types, 48, 75
 - over TCP/IP, 47, 72
 - questions regarding, 74–75
 - settings, 50
 - WINS use of, 47–48
- Netsh commands, 160
- Network access
 - controlling, 82
 - local, 84
 - methods for, 83–85
 - remote, 85
- Network access policies
 - NAP. *See* NAP
 - overview of, 82–83
- Network Access Protection. *See* NAP
- Network address translation, 154, 164
- Network address translation server, 4
- Network design
 - for NAP, 103–104
 - remediation segment, 104
 - trusted segment, 104
 - untrusted segment, 103
- Network Device Enrollment Service, 498
- Network drive, 264–265
- Network File System. *See* NFS
- Network Information System
 - description of, 384, 397
 - NIS+, 385
- Network load balancing, 677
- Network Location Awareness, 274
- Network policy server, 94–103
- Network security, 84
- Network with limited connectivity, 226–228
- Network Zone Rule, 282
- NFS
 - configuring services for, 390–391
 - definition of, 388
 - File Share, 392–393
 - installing services for, 389–390
 - Root Access Entry added to Share, 393–394
 - uses of, 397
 - Version 2, 388
 - Version 3, 388

- NIS, 385, 397
 NIS+, 385
 Non-Authoritative Restore of Directory Services, 721–722
 NPAS
 monitoring and maintaining of, 159–160
 overview of, 89–91
 NS, 16, 23
Nslookup, 44
- O**
 Object, 218
 Object level recovery, 723–730
 Object migration, 330–348, 395
 Online Certificate Status Protocol, 498
 Operation Masters, 271
 Operations master role holders, 221
 Operations Masters, 224–225, 251
 .org, 6
 Organizational units
 description of, 202–203, 240
 Group Policy Objects linked to, 269, 297, 306
 hierarchy of, 306
 O/S files, 718
 OS level patch management, 748–749
- P**
 PAM. *See* Pluggable Authentication Modules
 Parent domains, 6, 20
 Parent partitions, 593–594
 Password(s)
 credential caching, 449–450, 468–469
 migrating of, 344
 policies, 187–190, 410
 TPM, 444
 Password authentication protocol, 151
 Password export server, 337–338
 Password Replication Policies
 branch-specific caching, 472
 description of, 464–466
 designing of, 470–472
 full account caching, 471–472
 no account caching, 471
 storage of, 469–470
 summary of, 482
 Password-based cryptography standard, 501
 Patch management
 decision making regarding, 794
 description of, 744–745, 747–748
 Microsoft Update, 753–754
 OS level, 748–749
 patches, 751–753
 summary of, 790
 Path Rule, 282
 PDC Emulator
 description of, 225, 272, 334, 452
 in Kerberos authentication, 410
 preparing of, in source domain, 336–337
 Perimeter networks
 access path, 161–162
 components of, 164
 implementation of, 162–163
 overview of, 160–162
 schematic diagram of, 162
 Server Core, 164–166, 179–180
 Permissions
 certificate templates, 565–566
 scope filtering, 308–309
 Unix systems, 384, 396
 PIN authentication, 425
 PKI. *See* Public Key Infrastructure
 PKIView, 497
 Plug-and-Play devices, 142
 Pluggable Authentication Modules, 384
 Plug-n-play hardware, 313
 p-node, 48
 Point-to-point tunneling protocol, 152–153
 Policy-based quality of service, 291–292
 Ports, 179
 Positive answer, 14

- Pretty Good Privacy, 494
 Prime number theory, 505
 Principle of Least Privilege, 163
 Printer policies, 235–238
 Private key
 definition of, 494, 496, 503
 recovery of, 535
 storage of, 535
 .pro, 6
 PTR, 16
 Public key
 definition of, 494, 496, 503
 secret key agreement via, 512
 Public key cryptography
 authentication, 511–512
 security challenges associated with, 509–510
 standards, 500–505
 Public key encryption, 499–500
 Public Key Infrastructure
 application certificates, 526
 assigning roles in, 542
 authentication uses of, 494–495
 certificate authority. *See Certificate authority*
 certificate services
 application certificates, 526
 installing, 514–523
 machine certificates, 526
 mechanism of operation, 513
 user certificates, 525
 components of, 496–498
 confidentiality goals, 495
 description of, 492
 digital signatures. *See Digital signature*
 enrollments, 542–543
 Enterprise, 497
 function of, 495–496
 integrity goals, 495
 key pairs, 494, 496
 machine certificates, 526
 networks that use, 493
 nonrepudiation goals, 495
 on World Wide Web, 493–494
 private key, 494, 496
 public key, 494, 496
 purpose of, 569
 role assignments in, 542
 summary of, 569–570
 trust model, 527
 trusted third party, 493
 user certificates, 525
 Windows Server 2008 enhancements, 497–498
 Public Key Policies, 281
 Public names, 4
 PXE boot, 599

Q

- Quality assurance, 584–587
 Quality of service
 parameters for, 7
 policy-based, 291–292

R

- RADIUS
 Access Clients, 87–88
 Accounting DataStore, 88
 Authentication Database, 88
 Clients, 86, 88
 components, 87–89
 description of, 85–86
 infrastructure schematic, 87
 Proxy, 88, 104–105
 Server, 85–86, 88
 Read-only domain controllers
 added to existing forest, 453
 authenticated accounts on, 468
 computer accounts, 457–460
 configuring, 447–474
 credential caching, 449–450, 468–469
 description of, 8, 22, 190, 229

- DNS zones on, 452
- features of, 448–449
- full domain controller vs., 416–417
- Group Policy processing, 485
- indications for, 417
- installing, 452–457, 482
- Kerberos ticket account and, 450–451
- media used to install, 457
- password changes, 450
- Password Replication Policies
 - description of, 464–466
 - designing of, 470–472
 - storage of, 469–470
- prestaging, 457–460
- purpose of, 448
- security provided by, 406
- Server Core installation, 460–461
- summary of, 482
- SYSVOL replication on, 485
- Universal Group membership
 - caching on, 415–416, 484
- Real-time streaming protocol, 291
- Recovery
 - Directory Services, 719
 - object level, 723–730
 - Server, 717–719
- Recursive queries, 7, 13
- redircmp.exe, 270
- redirusr.exe, 270
- Referral answer, 14–15
- Regional domain controllers, 222–224
- Registration Authority, 529, 567
- Relative Identifier. *See RID*
- Relative identifier master, 221
- Remediation Server (NAP), 96
- Remote access
 - description of, 85
 - strategy implementation, 149–150
- Terminal Services. *See Terminal Services*
- Remote administration
 - Group Policy, 479
 - overview of, 474–475
 - Remote Desktop for administration, 475
 - Remote Server Administration Tools, 475–476
 - Telnet, 476–477
 - Windows Remote Management, 477–479
- Remote Authentication Dial-In User Servicer. *See RADIUS*
- Remote Desktop Connection
 - configuring, 139–145
 - launching of, 138–139
 - termination of, 138–139
- Remote Desktop Protocol, 114
- Remote office
 - domain controller in, 411–414
 - global catalog server in, 414–415
 - security risks, 447
- Remote Server Administration Tools, 475–476
- RemoteApp feature in Terminal Services, 117–122
- Removable media, 667–668
- Replication partners, 55–60, 72
- Request for Comments 1123, 39
- Resource forests, 359
- Resource records, 15–17
- Responses to DNS query, 14–15
- Restoring
 - branch office concerns, 407
 - Certificate Services, 538–541
 - Group Policy Objects, 276–279
- Restricted Groups, 289–290
- Restructuring
 - Active Directory Migration Tool for, 334
 - directory enabled applications, 358
 - GUID affected by, 332–333
 - indications for, 356–357
 - inter-forest, 330, 355, 357–358, 395
 - intra-forest, 330, 353–357, 395
 - SID affected by, 332–333
 - user passwords maintained during, 337–339

- Reverse lookup queries, 9–10
 Reverse lookup zones, 34
 RFC 1123, 39
 RID, 330
 Rivest, Shamir, and Adleman algorithm, 510
RODC. *See* Read-only domain controller
 Role Separation, 448, 472–474
 Root certificate authority, 529–530, 562, 573
 Routing tables, 227
 RSA algorithm, 510
 RSAT. *See* Remote Server Administration Tools
 RSoP, 300–303
- S**
- SACLS, 247–248, 252
 SAMBA, 330
 Scavenging
 database, 55
 DNS server, 35–38
 WINS server, 63, 73
 SCCM, 194, 218
 SCDPM, 407
 Schema Master, 221
 Scope filtering
 definition of, 308
 permissions, 308–309
 WMI filters, 310–312, 319
 SCVMM. *See* System Center Virtual Machine Manager
 Sealed storage, 418–419
 Secret key encryption, 499, 512
 Secure Socket Tunneling Protocol. *See* SSTP
 Security
 branch office concerns, 406–407
 data description of, 667
 Group Policy Control over removable media, 667–668
 remote office, 447
 server, 89
 Terminal Server, 113
 threats to, 586
 Security baselines
 definition of, 775
 description of, 745, 774–775
 Group Policy Object Accelerator Tool, 777–778
 Security group, 242
 Security Identifier. *See* SID
 Security Updates, 752
 Self Healing NTFS, 662
 Server. *See also* Windows servers
 global catalog. *See* Global catalog servers
 NAP-supported, 91
 network policy, 94–103
 roles of, 90
 security on, 89
 Terminal Services Licensing Role Service installed on, 123–124
 Server Backup, 701–715
 Server consolidation
 benefits of, 580
 description of, 583–584
 Server Core
 description of, 164–166, 179–180
 installation, 624–626, 716
 read-only domain controller installation, 460–461
 Server Isolation
 benefits of, 170
 overview of, 169–170
 schematic diagram of, 171
 strategy for, 172–174
 Server Manager, 30
 Server Message Blocks, 389

- Server virtualization
 - application compatibility, 596–597
 - applications management, 640–644
 - backup and, 716
 - child partitions
 - description of, 595
 - guest operating systems running in, 595–596
 - competition comparisons for, 626–628
 - configuration, 601–614
 - description of, 580–583
 - detailed architecture, 591–596
 - in development testing environments, 584–587
 - disaster recovery uses, 587–588
 - guest operating systems, 595–596
 - high availability and, 700–701
 - implementation-related issues, 582–583
 - managing of servers, 638–639
 - microkernel hypervisor, 590–591
 - Microsoft, 597–601
 - monolithic hypervisor, 588–590
 - parent partition, 593–594
 - in quality assurance environments, 584–587
 - summary of, 648–649
 - virtual assets, 652
- Service packs, 752
- Service Redundancy, 695–696
- Service ticket, 216
- Session key encryption, 512
- SHA. *See* System Health Agent
- Share and Storage Management Console, 664–665
- Shared secret key cryptographies, 500
- Shortcut trusts, 359–360
- Shutdown scripts, 293–294
- SID(s)
 - definition of, 330
 - restructuring effect on, 332–333
 - structure of, 331
 - types of, 342
- SID filtering, 335–336
- SID History
 - Attribute, 342–343
 - description of, 333
 - during group migration in ADMT, 341
 - resource access maintained during intra-forest restructuring using, 354
- Simple Object Access Protocol, 477
- Single copy clusters, 696
- Single sign-on applications, 409–410
- Site, 204–205
- Site link, 204–205, 231, 251
- Site link bridges, 233–234
- Site link objects, 231–233
- Site objects, 234
- Smart cards, 573–574
- SMB, 389
- SOA, 17
- SOAP, 361, 477
- Social engineering, 461
- SoftGrid Application Virtualization, 640, 651
- SoftGrid Sequencer, 643
- Software as a Service, 328
- SoHR. *See* Statement of Health Response
- Solution accelerators, 413–414
- Source domain, 336–337
- SP1, 599
- Special identity groups, 244
- Specialized Security/Limited Functionality, 777–778, 792
- Split-brain DNS design, 24–26
- Split-brain syndrome, 23
- SQL Server 2005, 631, 787
- SRV, 17
- SSH, 476
- SSTP, 154–159
- Standard zones
 - primary, 18
 - secondary, 18, 23
- Secure dynamic updates, 32

Standby Continuous Replication, 696
 Start of authority records, 17, 23
 Starter Group Policy Objects, 295–296
 Startup scripts, 293–294
 Stateless address auto configuration, 66
 Statement of Health Response, 93, 97
 Static IP addresses
 assignment message for, 31
 on DNS server, 31
 Storage Area Networks, 666–667
 Storage Explorer Console, 665–666
 Storage Manager for SANs Console,
 666–667
 Storage planning
 multipath I/O, 663–664
 Self Healing NTFS, 662
 Stub zone, 18, 23
 Subnet objects, 235, 251
 Subnets, 205
 Subordinate certificate authority,
 529–530, 562
 Symmetric key encryption, 499
 System Center Configuration
 Manager, 194, 218
 System Center Data Protection
 Manager 2007, 407
 System Center Operations
 Manager 2007, 789
 System Center Virtual Machine Manager
 Administrator Console, 632–634
 description of, 630–632
 managing of servers, 638
 migration support functionality of,
 636–637, 653
 optimization of, 631
 Self Service Web Portal, 634–635
 server placement by, 629–630
 summary of, 646
 Virtual Machine creation using, 637
 Virtual Machine Manager Library,
 635–636

Virtualization Management Console
 comparisons with, 639
 VMWare support, 644
 Windows PowerShell command-line
 interface, 634, 638, 645
 System Health Agent, 92–93
 System health models, 788–789, 792
 System Health Validators (NAP), 95
 SYSVOL replication, 485

T

Tape archiving, 407
 TCP/IP
 communication purposes of, 2
 description of, 65–66
 Telnet, 476–477
 Templates. *See* Certificate templates
 Terminal Server
 Advanced tab, 145
 Authentication Method for, 109
 Display tab, 140
 Experience tab, 143–145
 General tab, 139–140
 Local Resources tab, 140–141
 planning, 112–113
 plug-and-play device support, 142
 Programs tab, 143
 security issues, 113
 Terminal Services Licensing Role
 Service installed on, 123–124
 Terminal Services Licensing Server and,
 connectivity between, 131–134
 User Group access, 112
 Terminal Services
 Client Access Licenses, 107, 122, 134–135
 corporate desktop, 116–117
 deployment of, 115–116
 description of, 85, 105–106
 disconnection from, 139
 Gateway, 114–115
 Gateway console, 147

- licensing, 110–111, 122
 - nodes, 116
 - operating modes, 107
 - remote access strategy, 115–116
 - RemoteApp programs, 117–122
 - Session Broker, 114
 - strength of, 106
 - troubleshooting, 145–148
 - Terminal Services Licensing Manager, 148
 - Terminal Services Licensing role
 - activating, 125–131
 - description of, 110–111, 122
 - installing, 122–125
 - Terminal Server and, connectivity
 - established between, 131–134
 - Terminal Services Licensing Server
 - activating
 - overview of, 125–126
 - using Automatic connection method, 126–128
 - using telephone method, 130–131
 - using Web browser method, 129–130
 - Client Access License activation on, 135
 - domain applications, 136
 - forest applications, 136
 - implementation challenges, 137
 - installing, 122–125
 - publishing, 134
 - Terminal Server and, connectivity
 - between, 131–134
 - Terminal Services Configuration tool
 - used to specify, 133–134
 - upgrading to domain server, 137
 - workgroup applications, 136
 - Terminal Services Licensing Service, 135–137
 - Terminal Services Role
 - configuring, 107–113
 - description of, 107
 - TGS-REQ/REP, 216
 - Ticket granting ticket, 216
 - Time to Live, 52
 - Topology
 - Active Directory. *See Active Directory topology*
 - hub-and-spoke, 408–409
 - Transmission Control Protocol/Internet Protocol. *See TCP/IP*
 - Trusted People, 281
 - Trusted Platform Modules, 417–418, 669
 - Trusted third party, 493
- U**
- UDDI, 361
 - Universal group membership caching, 415–416, 484
 - Unix systems
 - attributes
 - configuring of, for Active Directory accounts, 387–388
 - storage of, 400
 - authentication on, 384–388
 - file system paths and permissions on, 383–384
 - Identity Management for, 386
 - NIS for authentication on, 385
 - permissions on, 384, 396
 - Pluggable Authentication Modules, 384
 - Update Rollups, 752
 - Updates
 - critical, 751
 - definition, 751
 - DNS, 32
 - Security, 752
 - Upgrading
 - Active Directory domain, 348–351
 - backward compatibility issues, 330
 - forest, 348–351
 - GUID affected by, 332–333
 - indications for, 329–330
 - inter-forest, 330, 355, 357–358
 - intra-forest, 330, 353–357
 - SID affected by, 332–333

User Acceptance Testing, 748
 User accounts, migrating of, 339, 343–345
 User Certificate Templates, 559–560
 User certificates, 525, 573
 User Datagram Protocol, 154
 User passwords, 337–339

V

Versioning, of certificates, 566–567
 Virtual LANs, 104
 Virtual machines
 configuring, with Hyper-V, 614–624
 System Center Virtual Machine Manager
 used to create, 637
 Virtual private network
 authentication protocols for, 150–152
 configuring connections for, 156–159
 description of, 85
 establishment of, 150
 L2TP/IPSec, 153–154
 point-to-point tunneling protocol, 152–153
 SSTP, 154–159
 Virtual resource management tool, 629
 Virtual Servers
 2005 R2, 597–599
 configuring, 614–624
 placement of, 628–630
 Virtualization. *See* Server virtualization
 Virtualization Management Console, 639
 Virtualization Role, 602–614
 Virtualization Service Clients, 594–595
 Virtualization Service Provider, 594
 Virtualized applications, 640–644
 VMBus, 594
 VMWare, 626, 644–645
 Volume encryption, 419, 421, 423–424
 Volume Shadow Copy Services, 702

W

WAN links, 223
 WBEM, 310
 Web browser, for activating Terminal Services Licensing Server, 129–130
 Web Enrollment, 497–498
 Web Services
 definition of, 328
 HTTP Protocol and, 361
 Security protocol, 361
 Trust protocol, 361
 Web-Based Enterprise Management, 310
 Window Server Backup Utility, 717–719
 Windows Firewall with Advanced Security, 166–169, 179, 290–291
 Windows Internet Naming Service.
 See WINS
 Windows NT4, 399
 Windows PowerShell
 description of, 303–306
 System Center Virtual Machine Manager
 2007 command-line interface, 634, 638, 645
 Windows Process Activation Service, 673
 Windows Recovery Environment
 Bare Metal Restore, 717–719
 description of, 717
 Windows Remote Management, 477–479
 Windows Scripting Host, 284
 Windows Server 2000
 domain function level, 211
 upgrading to Windows Server 2008
 Active Directory Domain Services, 213–214
 Windows Server 2003
 Active Directory integration in, 22
 domain function level, 211
 forest upgrade to Windows Server 2008, 214, 253
 Windows Server 2008
 Active Directory integration in, 22

- Active Directory Migration Tool for, 334
BitLocker installation on, 429–430
DNS enhancements in, 7–8
domain function level, 211
upgrade matrix for, 348
Virtualization Role installation on,
 602–614
Windows Server 2003 forest
 upgrade to, 214
Windows Server 2000 native mode Active
 Directory upgraded to, 213–214
Windows Server Update Services
 application patching, 774
 assignment of computers into, 794
 branch office deployment of, 755–756
 Clients, configuring of, 770–774
 configuring, 764–768
 deploying to client computers, 768–770
 description of, 749–750
 implementation of, 754, 758
 infrastructure, 754–758
 installing, 758–763
 in large enterprises, 756–758
 patches, 751–753, 795
 products updated with, 749–750
 in small enterprises, 754–755
 summary of, 791
 system requirements, 750–751
Windows SharePoint Services, 363,
 672–673, 675–676, 737
Windows System Resource Manager, 147
Windows Vista
 BitLocker installation on, 428
 Virtual Server 2005 R2 support, 600
- WINS
 clients, configuring information for,
 48–51
 description of, 23–24, 68–69
 NetBIOS protocol use by, 47–48
 summary of, 72–73
- WINS server
 burst handling, 60–62
 configuring, 53–56
 DNS server integration with, 44–45
 HOSTS file, 46–47
 installing, 53
 maintaining, 60–63
 name registration, 51–52
 nodes, 54
 replication partners, 55–60, 72
 scavenging records, 63, 73
 setting up, 52–53
- Wired workstations, 84
Wireless workstations, 84
Witness Disk, 678
WMI
 BitLocker interface, 437
 filters, 310–312, 319
- WS. *See* Web Services
- WSUS. *See* Windows Server Update
 Services
- X**
- X.509, 506–507, 545, 572
Xen-enabled Linux Kernels, 596
- Z**
- Zones. *See* DNS zones