



The Real

# MCITP Windows Server 2008 Server Administrator

## Exam 70-646

### 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

**Naomi Alpern**  
**Tariq Azad**

**Dustin Hannifin**  
**Shawn Tooley**

# 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](http://www.syngress.com/solutions). Once registered, you can access our [solutions@syngress.com](mailto: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](http://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](mailto: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](mailto:sales@syngress.com) for more information.

This page intentionally left blank

# **The Real MCITP Exam 646 Windows Server 2008 Server Administrator Prep Kit**

**Tony Piltzecker** Technical Editor

**Naomi Alpern  
Tariq Azad  
Dustin Hannifin  
Shawn Tooley**

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	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY

Syngress Publishing, Inc.

Elsevier, Inc.

30 Corporate Drive

Burlington, MA 01803

**The Real MCITP Exam 70-646 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: 978-1-59749-248-5

Publisher: Andrew Williams

Page Layout and Art: SPI

Acquisitions Editor: David George

Copy Editor: Michelle Huegel

Technical Editor: Tony Piltzecker

Indexer: Nara Wood

Project Manager: Gary Byrne

Cover Designer: Michael Kavish

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

# Contributing Authors

**Naomi J. Alpern** currently works for Microsoft as a consultant specializing in Unified Communications. She holds many Microsoft certifications, including an MCSE and MCT, as well as additional industry certifications such as Citrix Certified Enterprise Administrator, Security+, Network+, and A+. Since the start of her technical career she has worked in many facets of the technology world, including IT administration, technical training, and, most recently, full-time consulting. She likes to spend her time reading cheesy horror and mystery novels when she isn't browsing the Web. She is also the mother of two fabulous boys, Darien and Justin, who mostly keep her running around like a headless chicken.

**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, Comaq, 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.

**Dustin Hannifin** (Microsoft MVP—Office SharePoint Server) is a systems administrator with Crowe Chizek and Company LLC. Crowe ([www.crowechizek.com](http://www.crowechizek.com)), one of the nation's leading public accounting and consulting firms. Under its core purpose of "Building Value with Values®," Crowe assists both public and private companies in reaching their goals through services ranging from assurance and financial advisory to performance, risk, and tax consulting. Dustin currently works in Crowe's Information Services delivery unit, where he plays a key role in maintaining and supporting Crowe's internal information technology (IT) infrastructure. His expertise resides in various Microsoft products, including Office SharePoint Server, System Center Operations Manager, Active Directory, IIS, and Office Communications Server. Dustin holds a bachelor's degree from Tennessee Technological University and is a founding member of the Michiana IT Professionals Users Group. He regularly contributes to technology communities, including his blog ([www.technotesblog.com](http://www.technotesblog.com)) and Microsoft newsgroups. Dustin, a Tennessee native, currently resides in South Bend, IN.

**Shawn Tooley** owns a consulting firm, Tooley Consulting Group, LLC, that specializes in Microsoft and Citrix technologies, for which he is the principal consultant and trainer. Shawn also works as network administrator for a hospital in northeastern Ohio. Shawn's certifications include Microsoft Certified Trainer (MCT), Microsoft Certified System Engineer (MCSE), Citrix Certified Enterprise Administrator, Citrix Certified Sales Professional, HP Accredited System Engineer, IBM XSeries Server Specialist, Comptia A+, and Comptia Certified Trainer. In his free time he enjoys playing golf.

# Contents

<b>Foreword .....</b>	<b>xvii</b>
<b>Chapter 1 Planning for Server Deployment .....</b>	<b>1</b>
Introduction .....	2
Planning for Installation or Upgrade .....	2
Selecting a Windows 2008 Edition .....	3
Rollback Planning .....	5
Implementing BitLocker.....	10
Planning for Infrastructure Services.....	11
Address Assignment .....	12
Name Resolution (DNS) .....	20
DNS Zones.....	22
Reverse Zones .....	23
Planning For Global Naming Zones.....	23
DNS Records .....	24
Planning for Dynamic DNS (DDNS) .....	26
Scavenging .....	26
Planning For DNS Forwarding.....	26
Network Access Protection .....	27
Planning for NAP Enforcement Methods .....	27
Planning For DHCP NAP Enforcement.....	29
Planning For IPSec NAP Enforcement .....	29
Planning For 802.1x NAP Enforcement .....	30
Planning For VPN NAP Enforcement.....	30
Planning for NAP Servers .....	31
Health Policy Servers.....	31
Health Requirement Servers .....	31
Health Registration Authority Servers .....	31
Planning for NAP Clients .....	32
Directory Services .....	32
Planning Forests and Domains .....	33
Planning Domain Controller Placement .....	35
Planning Active Directory Sites and Site Links .....	36
Planning Organizational Unit Design .....	38
Delegating Authority to Organizational Units.....	39
Planning for Automated Server Deployment .....	42

Standard Server Image .....	53
Automation and Scheduling .....	54
Certificate Services.....	54
Introduction to Public Key Infrastructure .....	54
Planning Certificate Servers .....	55
Planning Root, Subordinate, and Intermediate Certificate Authorities.....	56
Planning Application Services .....	57
Planning for Web Applications.....	57
Web Farms and Web Site Availability.....	57
IIS Authentication Methods .....	58
IIS Delegation and Remote Administration.....	58
IIS 7 Core Server.....	59
FTP, POP3, and SMTP .....	59
Windows SharePoint Services 3.0.....	59
Planning for Virtualization.....	60
Planning for Availability .....	61
Resilience .....	61
Accessibility.....	62
Planning for File and Print Services .....	62
Working with Access Permissions .....	62
Share Level Permissions vs File/Folder Permissions .....	62
Providing Access to Users and Groups.....	63
Allow and Deny .....	64
Storage Quotas.....	69
Planning for Replication.....	69
Indexing Files.....	70
Storage Policies .....	70
Understanding Availability Options .....	71
File and Print Server Clustering .....	71
Publishing Printers .....	73
Summary of Exam Objectives.....	74
Exam Objectives Fast Track .....	74
Exam Objectives Frequently Asked Questions .....	76
Self Test .....	77
Self Test Quick Answer Key .....	81
<b>Chapter 2 Planning for Server Management .....</b>	<b>83</b>
Introduction .....	84
Developing a Management Strategy .....	84

Remote Administration . . . . .	85
Remote Desktop . . . . .	87
Server Management Technologies . . . . .	91
Windows Powershell . . . . .	91
Windows Deployment Services (WDS) . . . . .	92
Windows Reliability and Performance	
Monitor . . . . .	92
Server Manager . . . . .	93
ServerManagerCMD . . . . .	98
Delegating Administration . . . . .	99
Delegating Authority . . . . .	100
Delegating Active Directory Objects . . . . .	102
Application Management . . . . .	103
Planning a Group Policy Strategy . . . . .	107
Understanding Group Policy . . . . .	109
Types of Group Policies . . . . .	109
Local Group Policy . . . . .	110
Non-Local Group Policy Objects . . . . .	113
Preferences . . . . .	119
Network Location Awareness . . . . .	122
User . . . . .	123
Computer . . . . .	124
Planning for GPOs . . . . .	125
Site, Domain, and OU Hierarchy . . . . .	126
Group Policy Processing Priority . . . . .	128
Creating and Linking Group Policy Objects . . . . .	130
Creating Stand-Alone GPOs . . . . .	131
Linking Existing GPOs . . . . .	131
Creating and Linking at One Time . . . . .	133
Controlling Application of Group Policies . . . . .	134
Enforce . . . . .	134
Block Inheritance . . . . .	138
GPO Backup and Recovery . . . . .	140
Troubleshooting . . . . .	140
Group Policy Results and Group Policy Modeling . . . . .	141
Summary of Exam Objectives . . . . .	148
Exam Objectives Fast Track . . . . .	149
Exam Objectives Frequently Asked Questions . . . . .	151
Self Test . . . . .	153

SelfTest Quick Answer Key .....	160
<b>Chapter 3 Monitoring and Maintaining Servers.....</b>	<b>161</b>
Introduction .....	162
Patch Management.....	162
OS Level Patch Management .....	164
Windows Server Update Service.....	166
WSUS 3.0 SP1 Deployment on Microsoft	
Windows 2008 Server.....	169
Microsoft WSUS 3.0 Service Pack 1 Administration	
Console .....	183
Configure Microsoft WSUS 3.0 Service Pack 1 Automatic	
Updates for Clients .....	189
Application Patching.....	196
Monitoring for Performance.....	199
Monitoring Servers.....	202
Optimization .....	208
Event and Service Management .....	217
Trending and Baseline Analysis .....	220
Summary of Exam Objectives.....	223
Exam Objectives Fast Track .....	225
Exam Objectives Frequently Asked Questions .....	226
SelfTest .....	228
SelfTest Quick Answer Key .....	231
<b>Chapter 4 Security and Policies .....</b>	<b>233</b>
Introduction .....	234
Remote Access Security.....	235
Installing and Configuring NPAS .....	237
Routing and Remote Access Service.....	237
Network Interfaces .....	242
Remote Access Clients.....	243
Ports .....	244
PPTP .....	244
L2TP/IPsec .....	247
SSTP .....	247
Network Access Protection .....	248
Working with NAP .....	249
Network Layer Protection .....	249
NAP Clients .....	250

NAP Enforcement Points . . . . .	251
Active Directory Domain Services . . . . .	252
NAP Health Policy Server . . . . .	252
Health Requirement Server . . . . .	254
Restricted Network . . . . .	254
Software Policy Validation . . . . .	255
Server Security . . . . .	256
Windows Firewall Management . . . . .	257
Working with Built-in Firewall Exceptions . . . . .	261
Creating Manual Firewall Exceptions . . . . .	263
Advanced Configuration of the Windows Firewall . . . . .	267
Modifying IPsec Defaults . . . . .	270
Key Exchange (Main Mode) . . . . .	272
Data Protection (Quick Mode) . . . . .	273
Authentication Method . . . . .	274
Creating Connection Security Rules . . . . .	279
Configuring a Server-to-Server Connection	
Security Rule . . . . .	284
Creating Firewall Rules . . . . .	285
Monitoring the Windows Firewall . . . . .	290
Data Security . . . . .	291
BitLocker . . . . .	292
Encrypted File System . . . . .	294
Auditing . . . . .	295
Auditing AD DS and LDS . . . . .	296
Event Log . . . . .	298
Summary of Exam Objectives . . . . .	300
Exam Objectives Fast Track . . . . .	301
Exam Objectives Frequently Asked Questions . . . . .	303
Self Test . . . . .	305
Self Test Quick Answer Key . . . . .	308
<b>Chapter 5 Planning for Server Virtualization . . . . .</b>	<b>309</b>
Introduction . . . . .	310
Understanding Virtualization . . . . .	310
Server Consolidation . . . . .	313
Quality Assurance and Development Testing Environments . . . . .	314
Disaster Recovery . . . . .	317
Microkernelized vs. Monolithic Hypervisor . . . . .	318
Monolithic Hypervisor . . . . .	318

Microkernel Hypervisor . . . . .	320
Detailed Architecture . . . . .	321
Parent Partition . . . . .	323
Child Partitions . . . . .	325
Guest Operating Systems . . . . .	325
Guest with Enlightened Operating System . . . . .	325
Guest with Partially Enlightened Operating System . . . . .	326
Legacy Guest . . . . .	326
Application Compatibility . . . . .	326
Microsoft Server Virtualization . . . . .	327
Hyper-V . . . . .	330
Configuration . . . . .	331
Installing the Virtualization Role on Windows Server 2008 . . . . .	332
Configuring Virtual Servers with Hyper-V . . . . .	344
Server Core . . . . .	354
Competition Comparison . . . . .	356
Server Placement . . . . .	358
System Center Virtual Machine Manager 2007 . . . . .	360
Virtual Machine Manager Administrator Console . . . . .	362
Windows PowerShell Command-Line Interface . . . . .	364
System Center Virtual Machine Manager Self Service	
Web Portal . . . . .	364
Virtual Machine Manager Library . . . . .	365
Migration Support Functionality . . . . .	366
Virtual Machine Creation Process Using SCVMM . . . . .	367
Managing Servers . . . . .	368
Stand-Alone Virtualization Management Console . . . . .	369
Managing Applications . . . . .	370
Managing VMware . . . . .	374
Summary of Exam Objectives . . . . .	376
Exam Objectives Fast Track . . . . .	377
Exam Objectives Frequently Asked Questions . . . . .	381
Self Test . . . . .	384
Self Test Quick Answer Key . . . . .	387
<b>Chapter 6 Application and Data Provisioning . . . . .</b>	<b>389</b>
Introduction . . . . .	390
Provisioning Applications . . . . .	391
Terminal Server Infrastructure . . . . .	391
Terminal Server Licensing . . . . .	391

Terminal Services Gateway Server . . . . .	402
Terminal Services Session Broker . . . . .	409
Terminal Services RemoteApp . . . . .	413
Resource Allocation . . . . .	419
Microsoft Windows System Resource Manager . . . . .	420
Application Virtualization . . . . .	424
Microsoft SoftGrid Application Virtualization . . . . .	425
System Center Configuration Manager 2007 . . . . .	426
Introduction to SCCM . . . . .	427
Hardware Inventory . . . . .	436
Software Inventory . . . . .	439
Application Management and Deployment . . . . .	443
OS Deployment . . . . .	446
Provisioning Data . . . . .	447
Working with Shared Resources . . . . .	447
Offline Data Access . . . . .	449
Summary of Exam Objectives . . . . .	452
Exam Objectives Fast Track . . . . .	454
Exam Objectives Frequently Asked Questions . . . . .	456
Self Test . . . . .	458
Self Test Quick Answer Key . . . . .	461
<b>Chapter 7 Planning for Business Continuity and High Availability . . . . .</b>	<b>463</b>
Introduction . . . . .	464
Planning for Storage Requirements . . . . .	465
Self Healing NTFS . . . . .	466
Multipath I/O (MPIO) . . . . .	467
Data Management . . . . .	468
Share and Storage Management Console . . . . .	468
Storage Explorer . . . . .	469
Storage Manager for SANs Console . . . . .	470
Data Security . . . . .	471
Group Policy Control over Removable Media . . . . .	471
BitLocker Drive Encryption . . . . .	472
BitLocker Volume Recovery . . . . .	474
BitLocker Management Options . . . . .	474
Using BitLocker for the Safe Decommissioning of Hardware . . . . .	475
Data Collaboration . . . . .	476

Planning for High Availability . . . . .	481
Failover Clustering . . . . .	481
Architectural Details of Windows 2008 Failover Clustering . . . . .	482
Multi-Site Clusters . . . . .	498
Service Redundancy . . . . .	499
Service Availability . . . . .	501
Data Accessibility and Redundancy . . . . .	501
Failover Clustering . . . . .	502
Prerequisites . . . . .	502
Distributed File System . . . . .	503
Virtualization and High Availability . . . . .	504
Planning for Backup and Recovery . . . . .	505
Data Recovery Strategies . . . . .	520
Server Recovery . . . . .	521
WinRE Recovery Environment Bare Metal Restore . . . . .	522
Command Line Bare Metal Restore . . . . .	523
Recovering Directory Services . . . . .	523
Backup Methods for Directory Services . . . . .	523
Backup Types for Directory Services . . . . .	524
Recovery Methods for Directory Services . . . . .	524
Directory Services Restore Mode Recovery . . . . .	524
Non-Authoritative Restore . . . . .	525
Authoritative Restore . . . . .	527
Object Level Recovery . . . . .	527
Summary of Exam Objectives . . . . .	535
Exam Objectives Fast Track . . . . .	535
Exam Objectives Frequently Asked Questions . . . . .	540
Self Test . . . . .	543
Self Test Quick Answer Key . . . . .	546
<b>Appendix Self Test Appendix . . . . .</b>	<b>547</b>
Chapter 1: Planning for Server Deployment . . . . .	548
Chapter 2: Planning for Server Management . . . . .	553
Chapter 3: Monitoring and Maintaining Servers . . . . .	564
Chapter 4: Security and Policies . . . . .	568
Chapter 5: Planning for Server Virtualization . . . . .	572
Chapter 6: Application and Data Provisioning . . . . .	577
Chapter 7: Planning for Business Continuity and High Availability . . . . .	582
<b>Index . . . . .</b>	<b>589</b>

# Foreword

This book's primary goal is to help you prepare to take and pass Microsoft's exam number 70–646, *Windows Server 2008 Server 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 70–646?

Professional Series Exam 70–646 is the final requirement for those pursuing *Microsoft Certified Information Technology Professional (MCITP): Server Administrator* certification for Windows Server 2008. The server administrator is responsible for the operations and day-to-day management of an infrastructure of servers for an enterprise organization. Windows server administrators manage the infrastructure, Web, and IT application servers. Candidates for this certification are IT professionals who want to be known as leaders and problem solvers in a current or future role in an organization that uses Windows Server 2008.

However, not everyone who takes Exam 70–646 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 or management 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 70–646 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 for Server Deployment** This includes planning server installations and upgrades, planning for automated server deployment, planning infrastructure services server roles, planning application servers and services, and planning file and print server roles.
- **Planning for Server Management** This includes planning server management strategies, planning for delegated administration, and planning and implementing group policy strategy.
- **Monitoring and Maintaining Servers** This includes implementing patch management strategy, monitoring servers for performance evaluation and optimization, and monitoring and maintaining security and policies.
- **Planning Application and Data Provisioning** This includes data and application provisioning.
- **Planning for Business Continuity and High Availability** This includes planning storage, planning high availability, and planning for backup and recovery.



### 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](http://www.microsoft.com/learning/mcp/default.mspx) for the most updated information on each Microsoft exam.

Microsoft presently 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: Server Administrator* certification in any order, successful completion of the following MCTS exams is required for certification, in addition to Professional Series Exam 70–646:

- 70–640 *Configuring Windows Server 2008 Active Directory*
- 70–642 *Configuring Windows Server 2008 Network Infrastructure*



### Note

---

Those who already hold the MCSA or MCSE in Windows Server 2003 can upgrade their certifications to MCITP Server Administrator by substituting exam 70–648 (MCSA) or 70–649 (MCSE) for exams 70–640 and 70–642 above.

---

Preparation for this exam should include the following:

- Visit the Web site at [www.microsoft.com/learning/exams/70-646.mspx](http://www.microsoft.com/learning/exams/70-646.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/](http://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/70646](http://www.syngress.com/certification/70646).

## Exam Day Experience

Taking the exam is a relatively straightforward process. Prometric testing centers administer the Microsoft 70-646 exam. You can register for, reschedule, or cancel an exam through the Prometric Web site at [www.register.prometric.com](http://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 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 ones. 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](http://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 646

### Planning for Server Deployment

#### Exam objectives in this chapter:

- Planning for Installation or Upgrade
- Planning for Infrastructure Services
- Planning for Automated Server Deployment
- Planning for Application Services
- Planning for File and Print Services

#### 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 this chapter we will cover the various aspects of planning your Windows Server 2008 deployment. Whether you are upgrading existing servers or installing new ones, this chapter will help you understand the process to properly deploy Windows Server 2008.

This chapter will also help you plan your deployment of core infrastructure services such as DHCP, DNS, Directory Services, and Network Access Protection (NAP). We will then take a look at deploying server virtualization using Microsoft's new Hyper-V technology. We will wrap up the chapter by discussing availability planning and file and print services.

After reading this chapter you should be able to properly plan a Windows Server 2008 deployment following industry best practices and Microsoft guidelines. You should also be able to ensure a Server 2008 deployment is properly configured for supporting various core infrastructure components such as DHCP and DNS.

## Planning for Installation or Upgrade

The first step in planning your deployment is to decide if you will be upgrading your existing servers or deploying new hardware with a clean install of Windows Server 2008. The key difference between the two is that an upgrade simply replaces the old files on the current operating system (OS) with the new ones. By performing this process you don't lose any data on the OS drive. A clean install, on the other hand, requires formatting the current OS drive and installing the complete operating system fresh. This process will delete any data on the current OS drive. If you have not yet deployed any Windows servers in your organization, then this decision has been made for you as upgrading is not an option. If you choose to upgrade then you must also determine if the existing hardware will meet the minimum requirements to install Windows Server 2008. The following chart provides the Microsoft recommended requirements for installing Server 2008. If your servers do not meet these requirements you should consider a hardware upgrade as part of the Server 2008 deployment process. In that case you would need to perform clean installs. Table 1.1 provides the Microsoft-recommended hardware requirements to install Windows Server 2008.

**Table 1.1 Windows Server 2008 Hardware Requirements**

Processor	1 or more 2ghz or faster
RAM Memory	2GB or more
Disk Space	40GB or more

### Configuring & Implementing...

#### **Microsoft Assessment and Planning**

The Microsoft Assessment and Planning (MAP) Solution Accelerator allows you to review your current environment and inventory your current servers. The MAP accelerator creates reports that allow you to easily determine if your current servers will meet the system requirements for Windows Server 2008. You can download the MAP solution accelerator from Microsoft TechNet at: <http://technet.microsoft.com/en-us/library/bb977556.aspx>.

Choosing whether to perform a clean install or upgrade to Windows Server 2008 is a key planning decision that must be made prior to deployment. You should consider both options carefully before proceeding with your Windows Server 2008 deployment. System requirements could play a key role in the upgrade/clean install decision depending on the age of your hardware. After figuring out whether to upgrade or install clean you will need to decide which edition of Server 2008 to deploy.

## **Selecting a Windows 2008 Edition**

Windows Server 2008 now comes in eight editions, compared to four editions offered in Windows Server 2003. The different editions offer different feature sets along with different price tags. Before deploying Windows Server 2008 you must closely consider the needs of your organization. You may find that Standard edition meets all your requirements or you may decide certain applications require the Enterprise edition of Server 2008. Table 1.2 outlines the eight editions of Windows Server 2008 and a few of the major differences between them. All editions except Itanium edition come in 32bit or 64bit versions.

**Table 1.2** Windows Server 2008 Editions Comparison

Feature	Standard	Enterprise	Datacenter	Web	Itanium	Standard w/Hyper-V	Enterprise w/Hyper-V	Datacenter w/Hyper-V
IIS 7.0 Web Server	X	X	X	X	X	X	X	X
Server Virtualization						X	X	X
Automatic Server Deployment	X	X	X			X	X	X
Server Core	X	X	X	X		X	X	X
Active Directory (Domain Controller)	X	X	X			X	X	X
BitLocker	X	X	X		X	X	X	X
PowerShell	X	X	X	X	X	X	X	X
Clustering		X	X				X	X

## Configuring & Implementing...

### Virtualization Licensing

When deciding which edition of Server 2008 to purchase, you should consider Microsoft's virtualization licensing policy. For example by purchasing a Windows Server 2008 Enterprise license you can run up to four virtualized instances of Server 2008 without needing to buy any additional OS licenses. You should also note that Windows Server 2008 will be available without Hyper-V at a slightly reduced cost. More info on Windows Server 2008 pricing and licensing can be found at <http://www.microsoft.com/windowsserver2008/en/us/pricing.aspx>.

# Rollback Planning

At some point during your deployment it may be important to reverse your changes to the environment due to configuration issues, application incompatibility, or other unforeseen situations. You should always spend adequate time preparing a rollback plan when making configuration changes to a production server environment. Upgrading to Windows Server 2008 is no exception. For example, what happens if you suddenly have a power outage, or even worse, hardware failure while upgrading the server's operating system? What if that same server hosts thousands of files? You need a way to get back. Unfortunately you won't have the option of clicking the "undo" button. However, there are steps you can take to minimize the risk of upgrading. The first and most important step is to ensure you have a good backup of all end user data and preferably the existing operating system. You can use one of several third-party backup utilities or simply use the backup utility built into Windows 2000 Server or Windows Server 2003.

## EXERCISE 1.1

### INSTALLING WINDOWS SERVER 2008

Now that we've made a backup of our current server, let's install Windows Server 2008. In our example we will be performing a clean install; however, the steps to perform an upgrade are similar. To install Windows Server 2008 perform the following:

1. Place the Windows Server DVD into the server's DVD drive and reboot or power on the server.
2. The system should find that the DVD is bootable and begin booting off of the CD. You may be prompted to **Press any key to boot from CD**. If you receive this prompt simply press a key to confirm you do want to boot from the installation DVD.
3. The Windows Server 2008 Setup wizard will start as soon as the DVD boots.
4. Choose your preferred **Language, Currency, and Keyboard** as seen in Figure 1.1. Then click **Next**.

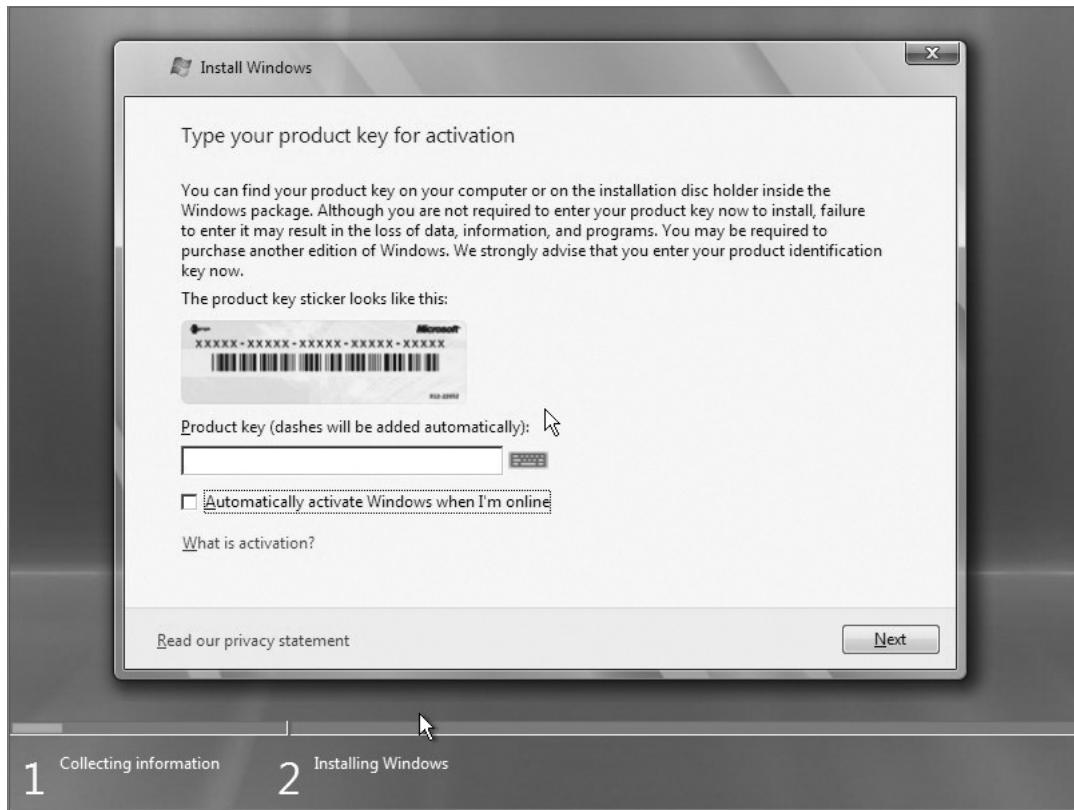
**Figure 1.1 Preferred Language**

5. Click the **Install Now** button as seen in Figure 1.2.

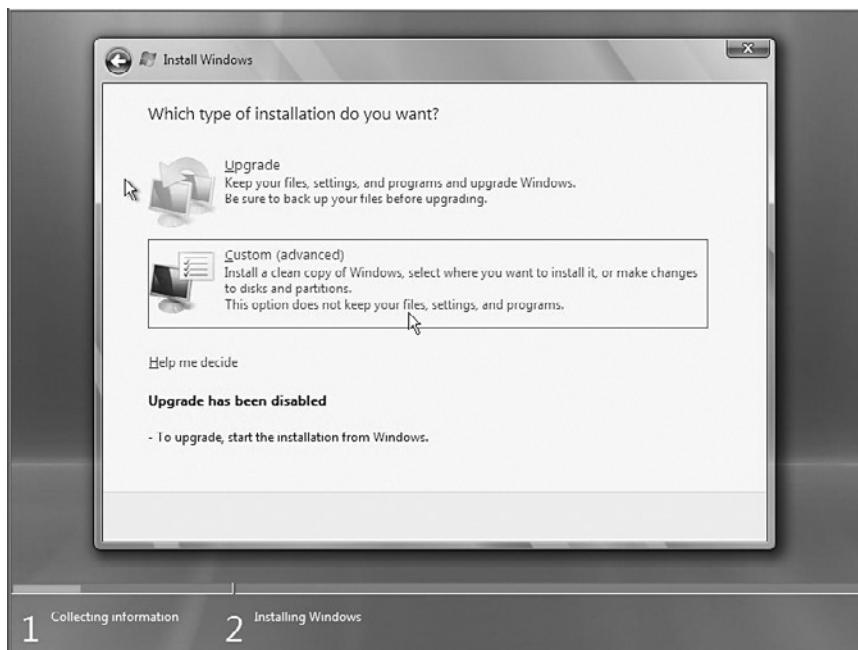
**Figure 1.2 Windows Server 2008 Setup Wizard**

6. Enter the product key for the edition you are installing (See Figure 1.3) or leave the product key field blank to install Windows Server 2008 in evaluation mode, then click **Next**.

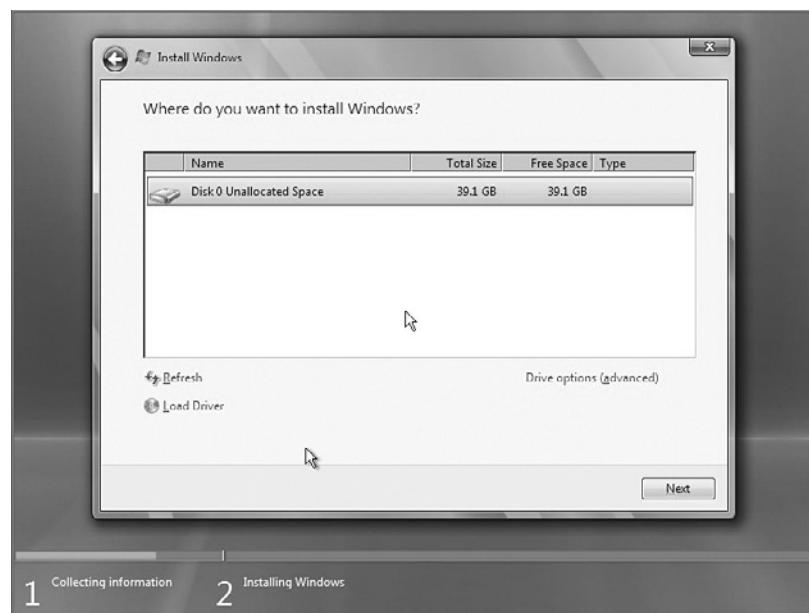
**Figure 1.3** Setup Wizard Product Key



7. Accept the license agreement, then click the **Next** button.
8. Since we booted from the DVD, and did not run setup from within an existing version of Windows, we do not have the option to upgrade. Go ahead and click the **Custom (advanced)** option as seen in Figure 1.4.

**Figure 1.4** Install Windows—Choose Installation Type

9. Choose the disk drive where you wish to install Windows Server 2008 (See Figure 1.5) then click the **Next** button.

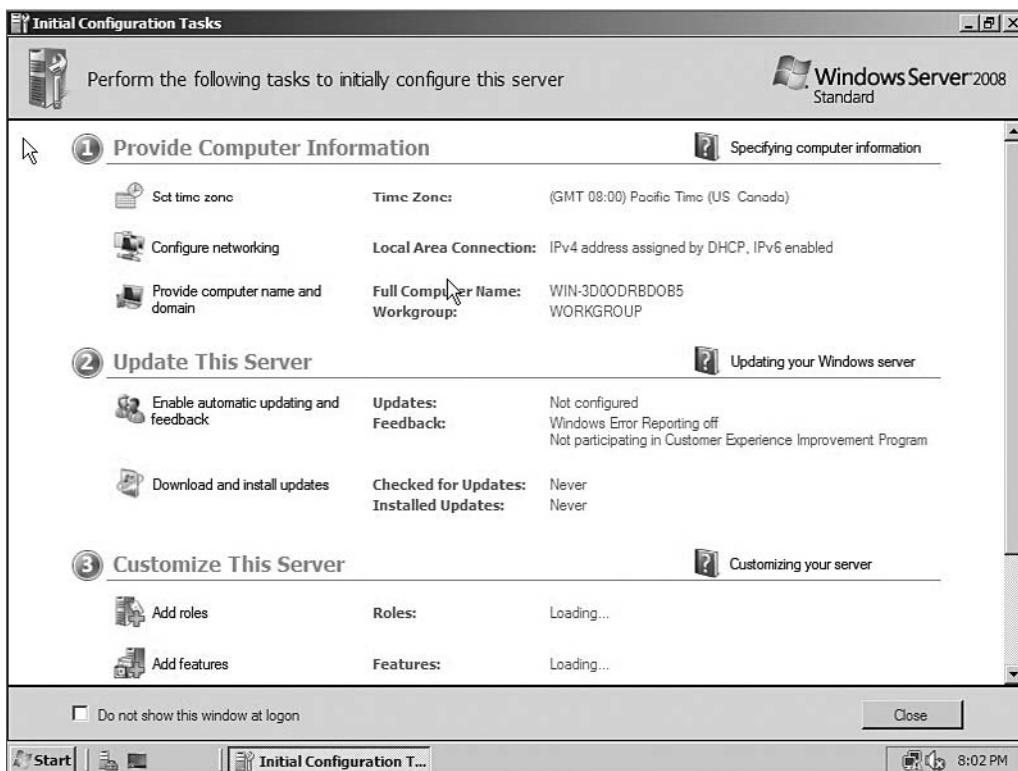
**Figure 1.5** Choose Drive Installation Drive

10. The Setup Wizard will perform the installation tasks as seen in Figure 1.6.

**Figure 1.6 Windows Server 2008 Install Progress**



11. After Windows is installed the server will reboot. At first boot you will be asked to change the Administrator password. Go ahead and change that to a secure password that you will remember.
12. After changing the Administrator password you will be logged into Windows. The initial configuration tasks console will launch. Go ahead and complete the assigned tasks to finish configuring the operating system (See Figure 1.7).

**Figure 1.7** Windows Server 2008 Initial Configuration Tasks

## Implementing BitLocker

Microsoft first introduced BitLocker with the release of Windows Vista. BitLocker provides true disk level encryption to help secure data on the computer in which it is installed. BitLocker is now a feature available in Windows Server 2008. By using BitLocker you can ensure the data on server disk drives is completely encrypted. If you are familiar with previous Windows operating systems, you are probably aware that you could easily physically pull a hard drive from one server and place it in another. You would then have the ability to access the data on that hard drive. This poses obvious security concerns for servers that could be placed in insecure locations. Someone could steal the server and place the hard drive in another computer. They would then be able to access the data on that drive. BitLocker addresses this problem by encrypting data on the physical disk. If encrypted with BitLocker, you cannot move the disk to another server and access it without the encryption key. By using BitLocker, servers located in insecure locations are much less likely to be accessed by someone unauthorized.

to do so. When planning your Windows Server 2008 deployment, you should consider on which servers you want to implement BitLocker. These servers typically would reside in an insecure location outside of your main datacenter; however, you may choose to use BitLocker on all servers and use disk encryption as part of your standard server deployment. Before we jump in and install BitLocker, there are some prerequisites you should be aware of. For BitLocker to be installed properly you will need:

- **Two Disk Volumes** You will need two volumes that must be set up during Windows installation. One volume hosts the Windows Server 2008 Operating System. The other is to provide an unencrypted space to initiate the boot process. The unencrypted volume should be 1.5GB or larger. If you choose to add another volume after Windows installation, you will need to reinstall Windows before using BitLocker.
- **TPM** BitLocker Requires a TPM compatible BIOS or an external USB storage device.

## Planning for Infrastructure Services

Planning for the deployment of Infrastructure Services provided by Windows Server 2008 is just as important as the server deployment itself. The services in this section require careful planning and proper configuration to function properly on your network. It is very important to understand what each service is doing on your network. It is equally important to understand and manage the configuration of that service.

### Head of the Class...

#### The Importance of Properly Planning Your Infrastructure Services

It is very critical that you take the time to clearly understand the infrastructure components provided by Windows Server 2008. Improper configuration or management of these services could cause major havoc on your network, or in a worst case scenario, render your Windows Server network useless.

For example, let's say you have an existing Windows Server 2003 DHCP Server on your network. DHCP (Dynamic Host Configuration Protocol) will

Continued

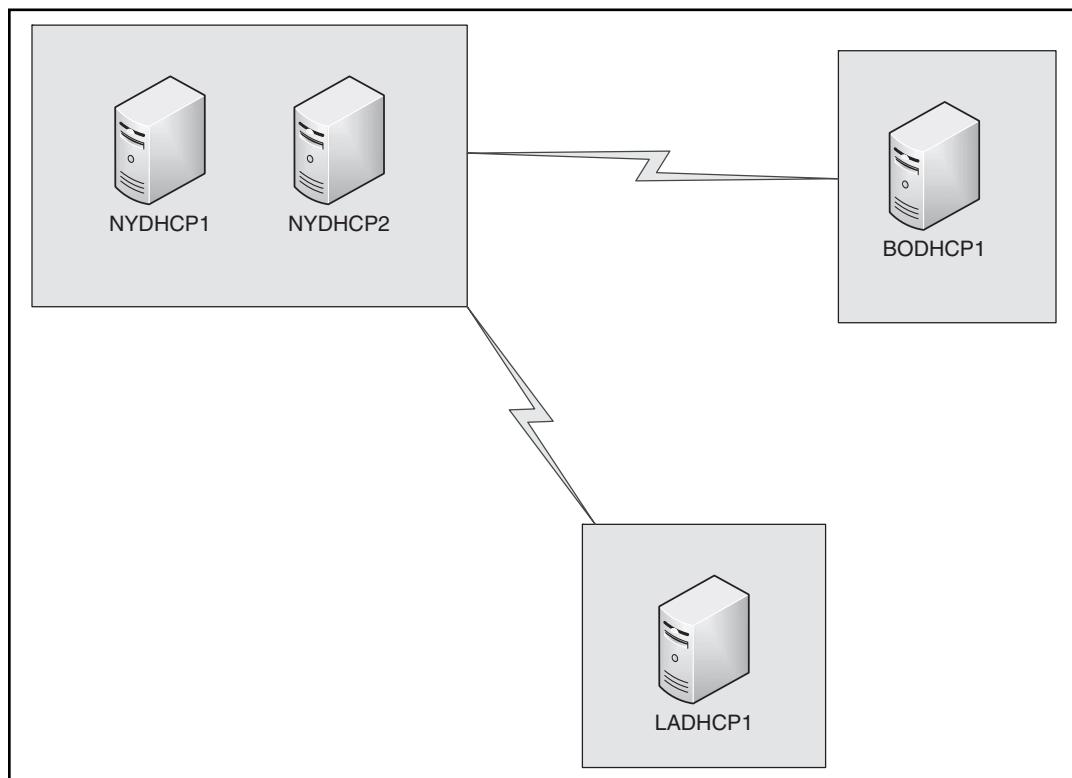
automatically assign IP addresses to computers and devices set to use DHCP for their IP configuration. Now let's pretend someone wrongly configures DHCP to provide the wrong range of IP addresses. By a simple click of the mouse any new computer placed on that network segment will no longer be able to access the Internet, browse file shares, or check e-mail. This simple misconfiguration could even cause client computers on that network to be unable to log on altogether.

Anyone with a little knowledge of Windows can install the OS, join it to a domain, and completely misconfigure the rest of the system and cause no problems to your network. However, if that same person improperly configures infrastructure services on that server, your network may become unstable and possibly un-useable.

## Address Assignment

Windows Server 2008 provides the Dynamic Host Configuration Protocol (DHCP) as an optional server role. This role allows the server to automatically assign IP addresses to computers throughout your organization. Without DHCP you would have to manually enter the IP address for each computer on your network. When deploying DHCP you must also take the number of network segments you have into consideration. Since DHCP uses a process that relies on broadcasts, it does not typically cross network routers. Since DHCP traffic cannot pass through a router you must plan to deploy a DHCP server on each network segment. The diagram in Figure 1.8 depicts a typical DHCP configuration. The example company below has three offices. The main office is located in New York City with two branch offices located in Boston and Los Angeles. The branch offices connect to the main office via the company's wide area network thus need DHCP servers deployed at that location. Now that you are familiar with a typical DHCP deployment let's walk through installing and configuring DHCP on Windows Server 2008.

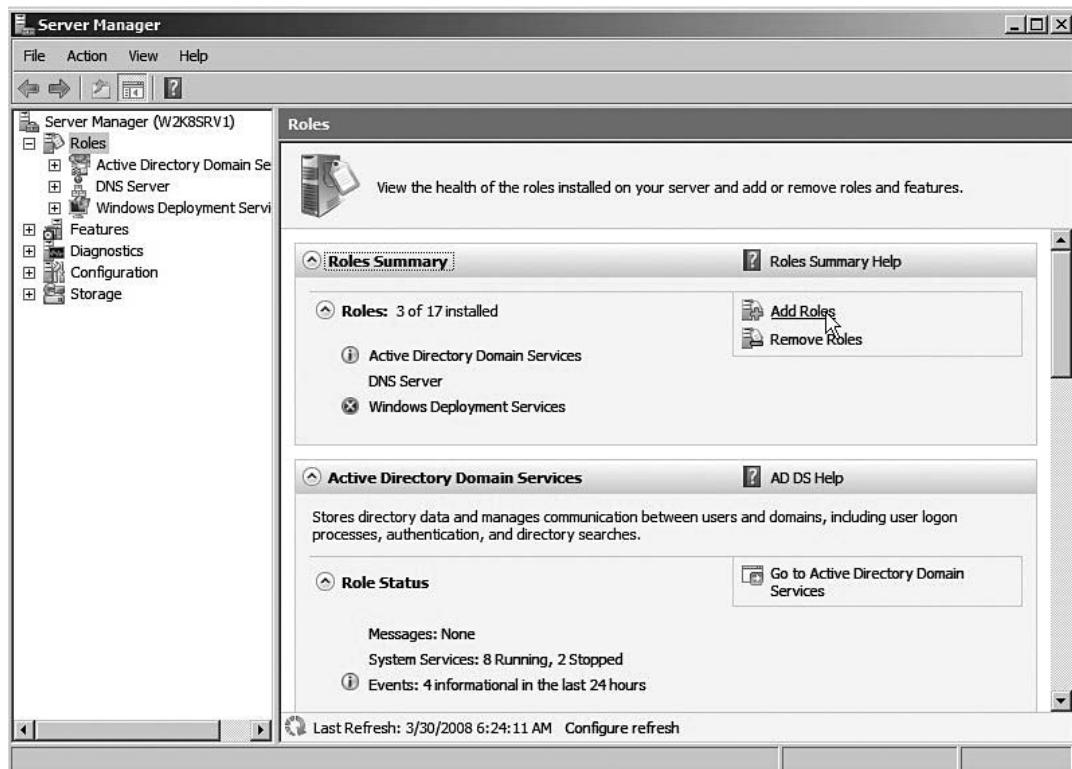
**Figure 1.8** Typical DHCP Deployment



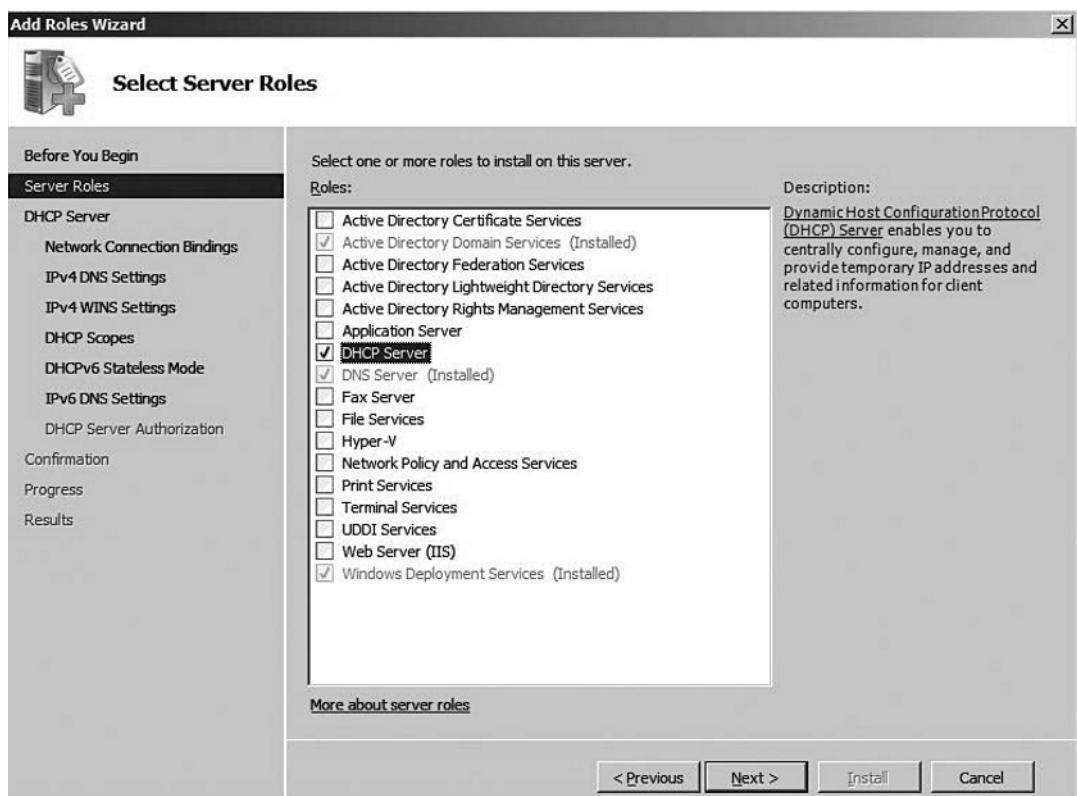
## EXERCISE 1.2

### INSTALLING AND CONFIGURING DHCP

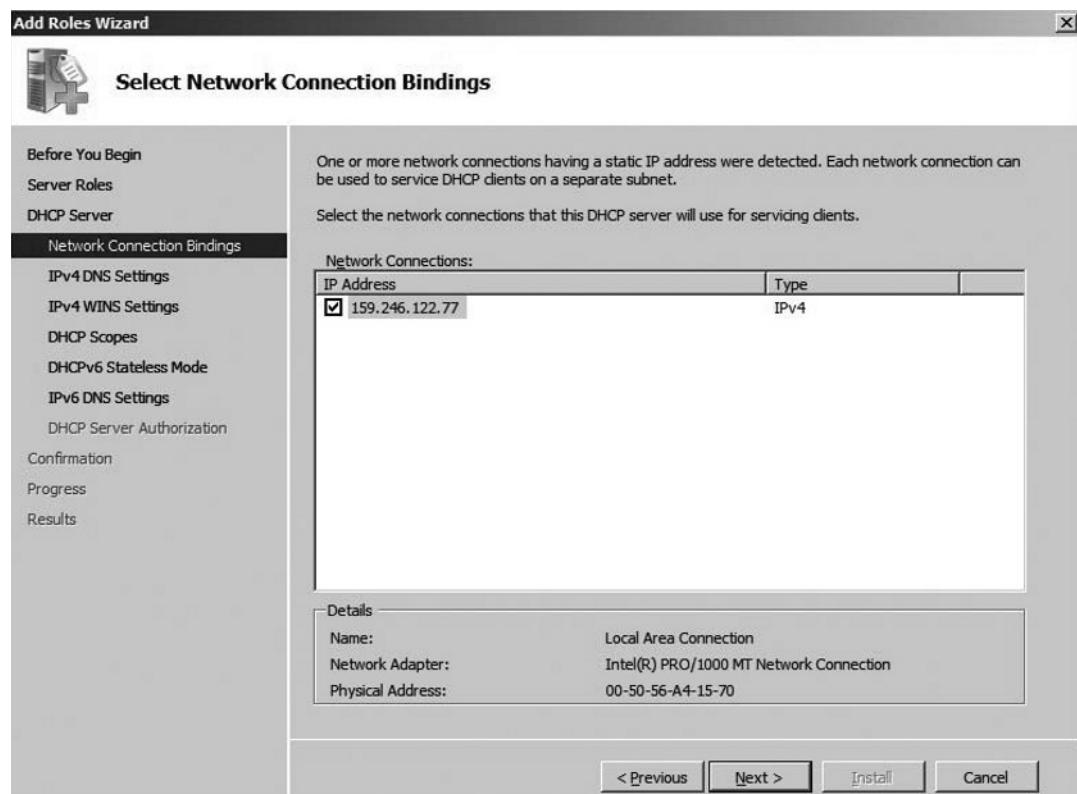
1. Open Server Manager by going to **Start | Administrative Tools | Server Manager**.
2. Click the **Roles** node.
3. Locate the **Add Roles** link in the center pane as seen in Figure 1.9.

**Figure 1.9 Add Role**

4. The **Add Roles** wizard will launch. Click the **Next** button to continue.
5. Click to select the **DHCP Server** role, as seen in Figure 1.10. Then click the **Next** button to continue.

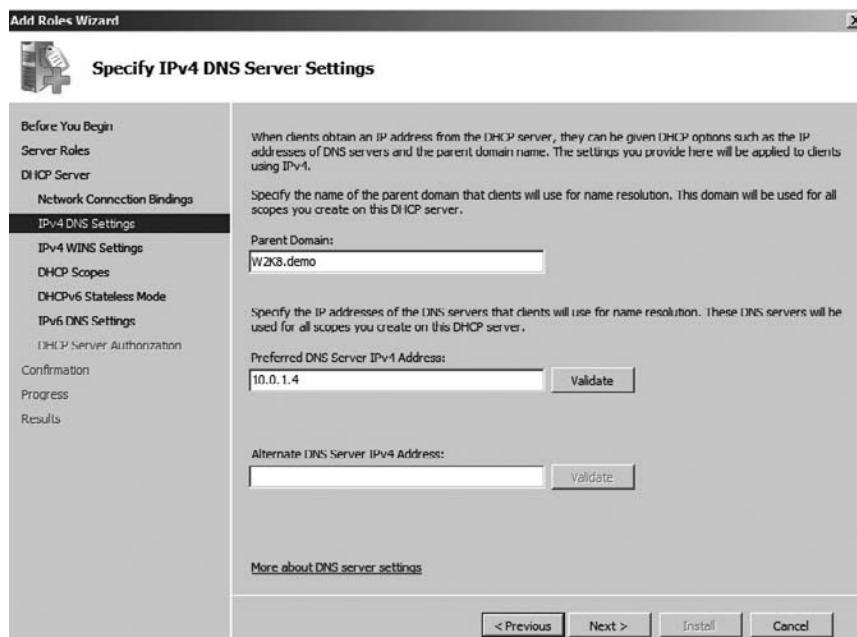
**Figure 1.10** Select DHCP Server Role

6. At the **Introduction to DHCP** screen, click the **Next** button to continue.
7. Select the network interface that you wish to bind to the DHCP service (See Figure 1.11). This is the network connection DHCP will use to assign IP addresses to clients. Then click the **Next** button to continue.

**Figure 1.11 Select Network Connection Bindings**

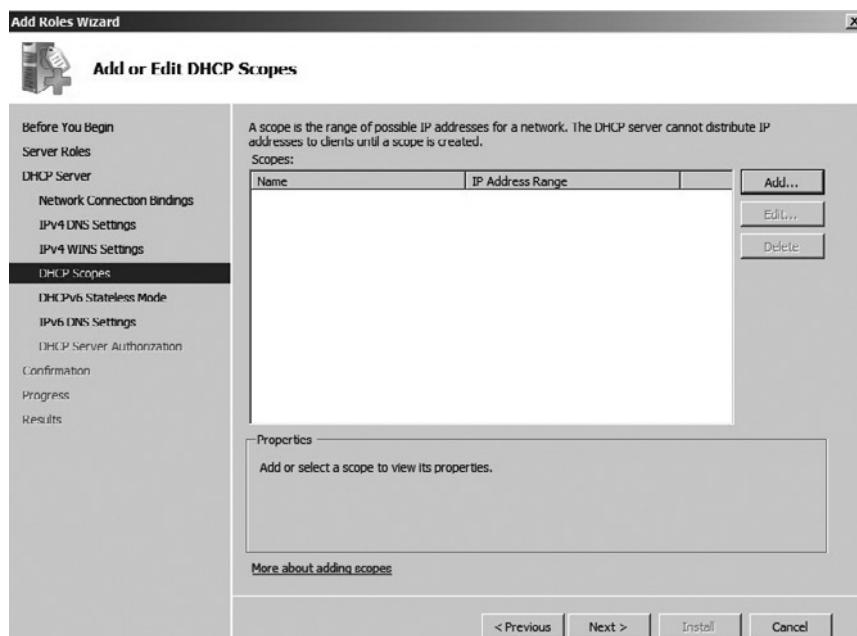
8. We now need to configure the settings that the DHCP server will provide to DHCP clients. We must configure DNS servers and default gateway settings that will be assigned to the clients. We also need to provide a range of IP addresses to offer to clients. Let's start by configuring the primary and secondary DNS servers as seen in Figure 1.12. Then click the **Next** button.

**Figure 1.12 DNS Server Settings**



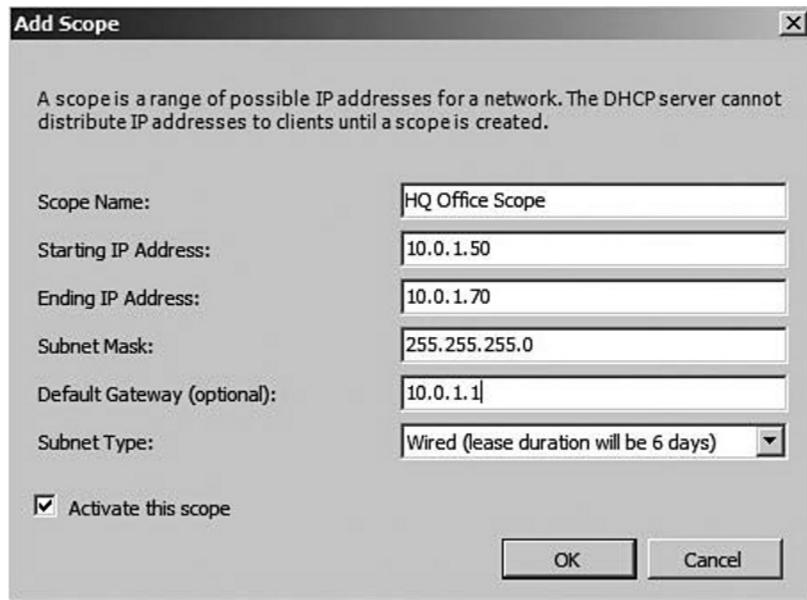
9. Now we'll set up the scope or range of IP addresses to offer to clients. Click the **Add** button as seen in Figure 1.13.

**Figure 1.13 DHCP Server Scope**

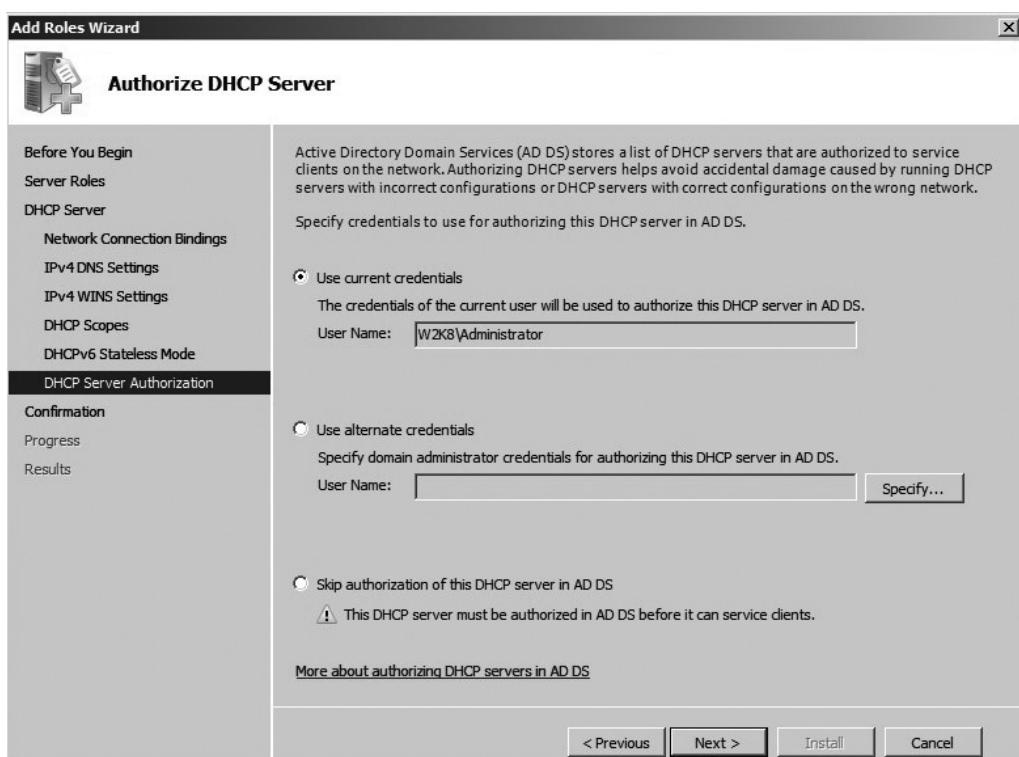


10. Enter the **Starting IP Address** and **Ending IP Address** to provide a range of addresses that will be offered to DHCP clients. Then enter the **Subnet Mask** and **Default Gateway** for the network segment. Finally set Subnet type which configures the lease time for addresses and ensure the **Activate This Scope** option is selected (See Figure 1.14). Then click the **OK** button.

**Figure 1.14** DHCP Scope Options



11. After returning to the **Add Roles** wizard go ahead and click the **Next** button to continue.
12. If you want to set up DHCP for an IPv6 network, you can do that at this step. However, if you are only setting up DHCP for IPv4, select the **Disable DHCPv6 stateless mode for this server** then click the **Next** button.
13. We must not authorize our DHCP server with Active Directory (AD). By requiring authorization, rogue DHCP servers can be prevented from offering IP addresses on your network. To authorize our DHCP go ahead and select the option to **Use current credentials** then click the **Next** button (See Figure 1.15).

**Figure 1.15** Authorize DHCP Server

14. On the summary screen, confirm that the options you chose are correct, and then click the **Install** button. DHCP will now be installed on the server. After installation completes you should be prompted with a success message. After you see that DHCP was successfully installed click the **Close** button.

### EXAM WARNING

Watch out for questions regarding the 80/20 rule for Windows Server DHCP servers. Microsoft recommends placing at least one redundant DHCP server on each network segment. This ensures IP addresses can be assigned to computers in the event that the primary DHCP server fails. Traditionally Microsoft has recommended that 80% of your available IP addresses be placed on the primary server, while 20% of those addresses are placed on the secondary server. More recently Microsoft has suggested using either an 80/20 type configuration or a 50/50 configuration.

## Name Resolution (DNS)

Windows Server 2008 networks rely extensively on the Domain Name System (DNS). It is important to understand how to set up, configure, and manage DNS before deploying a Server 2008 network. In this section we will discuss how to properly plan for and set up DNS.

You should first have a basic understanding of how DNS works. DNS was developed to provide name resolution for IP addresses. When the pioneers of TCP/IP networks were first developing the concept, they needed a way to uniquely identify each computer on the network. They decided each computer would be given a unique number-based address we now commonly refer to as an IP address. This concept poses obvious problems when humans try to access a computer on the network. They have to remember the numbered address for that computer. For example, can you imagine remembering the IP address of every Web site you want to visit? After all, those Web sites run on a very large TCP/IP network known as the Internet. Imagine remembering `http://155.212.56.73` to access the Syngress Web site. The numbered address concept obviously created a serious problem as TCP/IP networks grew. A few solutions have been developed over the years to try and address this problem. Ultimately DNS prevailed as the most efficient and manageable answer to the problem. DNS was developed to allow us to remember a name instead of the numbered address of a server. DNS is the service that translates `www.syngress.com` to `http://159.212.56.73`. Since many Windows services rely on name instead of number, DNS becomes a critical component in almost all networks.

Before jumping into planning DNS, you should have a brief understanding of how the DNS name resolution process works. DNS name resolution is done by a method known as querying, or performing a lookup query. A typical forward lookup query occurs as described below:

1. The client queries its local DNS server. For example, the client sends a query for `www.syngress.com`.
2. The local DNS server will then check to see if it contains the zone and has the authority to perform name resolution for that zone. If it does then it performs a lookup in the zone database and returns the IP address of the requested host to the client. If the DNS server cannot perform name resolution, it passes the query to a root DNS server. In our example we will

assume our local DNS server cannot resolve www.syngress.com. Our local DNS server would pass this request to a root DNS server, which would return a referral to the .com name servers.

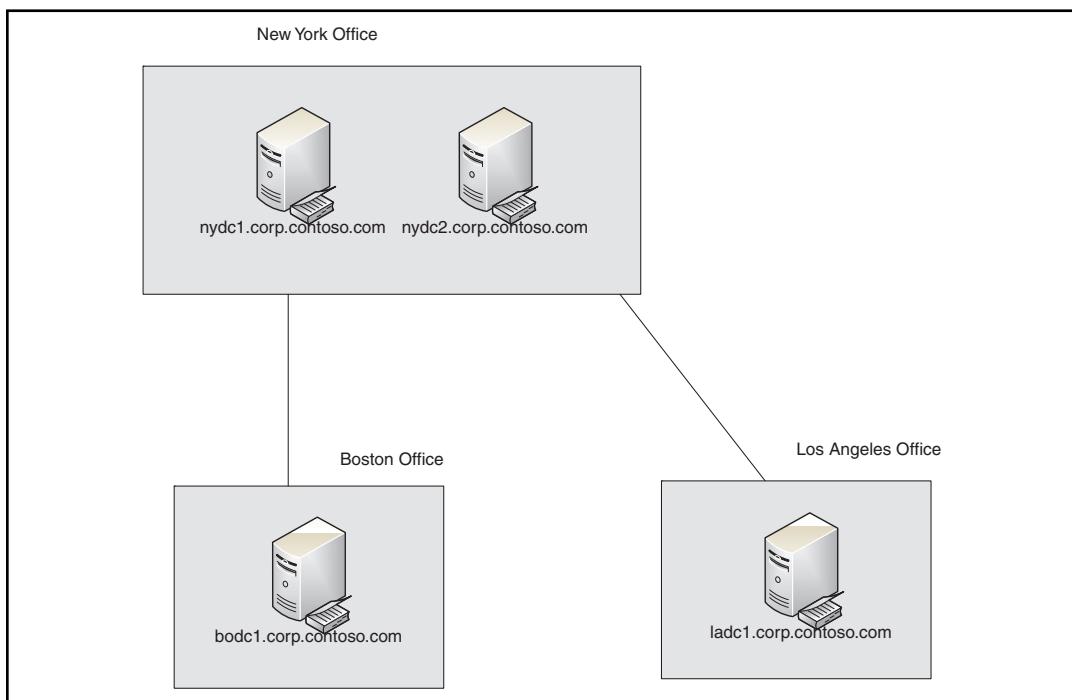
3. Our local DNS server would then send the query to the .com DNS servers which would return another referral to the Syngress authoritative DNS servers.
4. Our server would then send the initial query directly to the Syngress DNS servers. The Syngress DNS servers would respond with the IP address for www.syngress.com.

You should now have a basic understanding of how DNS name resolution works. Let's take a deeper look at planning for DNS.

### **EXAM WARNING**

DNS servers are often referred to as Name Servers (NS). If you see questions that discuss Name Servers you should be aware that they are referring to DNS Servers. The two are regularly used interchangeably.

When you are planning for DNS, one of the most important decisions to make is how many DNS servers you need on your network. Redundancy is always a must when planning your DNS deployment. At a very minimum you should have two DNS servers on your network. However in most Active Directory networks you have a larger number of DNS servers. Figure 1.16 depicts a typical Active Directory DNS deployment. Notice that the DNS zone corp.contoso.com is integrated with Active Directory so the primary zone is replicated to all DCs via AD replication. Workstations in each office would use the local DNS server to perform name resolution, but could also have one or both of the New York DNS servers as a secondary name server. If the local office DNS server failed, clients could contact a New York DNS server for name resolution.

**Figure 1.16** Typical Active Directory Integrated DNS Server Deployment

## DNS Zones

When planning your DNS deployment you must also consider how many DNS zones or domains are required for your infrastructure. You may need to have multiple zones to delegate security and management of part of your name space, you may need to plan for high availability and redundancy, or you simply may need to optimize performance for larger zones. All of these issues must be carefully reviewed when planning your DNS deployment. A DNS zone is the container that holds records (discussed later in this section). DNS zones typically are named according to the domain name in which they maintain records. For example the contoso.com zone would hold and maintain records for the contoso.com domain. For a medium-sized internal DNS deployment used to support Active Directory, you may only have a single DNS zone. A DNS server facing the Internet, used to host domains for your corporate Web site may have many DNS zones. When you have multiple DNS servers for redundancy you must have a way to transfer or replicate changes to all DNS Servers. Below is a brief description of the types of DNS zones available in Windows Server 2008.

- **Primary Zone (Stored in Active Directory)** Primary zones are created and updated directly on that server. Primary zones that are stored in Active Directory (AD) can also be replicated via normal AD replication. This is a very efficient way (and Microsoft recommended best practice method) to replicate DNS zones within your corporate network. It should also be noted that Active Directory integrated zones allow for multi-master updates. This means updates can take place in a secure fashion on any DC that the zone is replicated too.
- **Primary Zone (Standard)** Primary zones that are stored in a file on the server and secured by NTFS permissions. Like AD integrated primary zones, standard primary zones can be updated on the server that hosts them.
- **Secondary Zone** Secondary zones are read-only copies of primary zones. A secondary zone can be used to help load-balance traffic but must have updates performed on the primary zone servers.
- **Stub Zone** Like secondary zones, stub zones are read-only copies of primary zones. However, stub zones can be stored in AD like primary zones and contain only Name Server (NS), Start of Authority (SOA), and host (A) records for name servers.

## *Reverse Zones*

Reverse DNS zones are used to do the exact opposite for the standard Forward lookup zones. Reverse lookup zones provide the ability to find the fully qualified domain name (FQDN) of a host based upon its IP. For example, if you knew the IP address of 10.4.3.2, you could perform a reverse DNS query and find out that the hostname is server8.mydomain.com.

## Planning For Global Naming Zones

NETBIOS was the primary name resolution method used by Windows networks prior to DNS. Many Windows networks and applications still rely on NETBIOS. NETBIOS uses Windows Internet Naming Service (WINS) to assist in name resolution. Microsoft continues to encourage organizations to move away from NETBIOS-based name resolution and WINS, but many companies still have mission-critical line-of-business applications that rely heavily on this protocol.

To assist organizations in moving away from WINS, Microsoft has included Global Naming Zones (GNZ) in Windows Server 2008. GNZs allow administrators that still require NETBIOS name resolution to decommission WINS and move completely to DNS. GNZs hold single records that map NETBIOS names to IP addresses.

GNZ records must be updated manually. If you have NETBIOS names that update on a regular basis you may need to keep WINS around and use a combination of the two services.

## DNS Records

DNS Records are what you might consider the “data” of DNS. DNS records are what map IP addresses to host names. There are also several specialized DNS records that hold configuration information for the zone itself. Some of the most common DNS records are listed below:

- **A (Host) Record** A records are basic records used to map IP addresses to host names. These are the most commonly used records in DNS. For example, an A record would be used to map server1.contoso.com to 10.2.3.4.
- **CNAME (Alias) Record** CNAME records are also known as alias records. CNAME records map a host name to an existing A record. For example a CNAME record could map www.syngress.com to webserver1.syngress.com. Alias records are a great way to map Web site domain names to particular server names. For example, you may have a Web server named web1.contoso.com. Let’s assume you already have an A record created for this Web server. You want to launch a new e-commerce Web site on this server and want to use a custom URL of <http://companystore.contoso.com>. You could obviously create another A record named companystore.contoso.com and map that to the IP address of the Web server. However, if you needed to change the IP address of the server, then you would have to update all host records pointing to that server. By using CNAME records for all Web site URLs, you would only need to update the one A record for the server. You should carefully plan and evaluate when to use CNAME records when deploying your DNS infrastructure.
- **MX (Mail Exchanger) Record** MX Records are used to map a domain name to an existing A record for mail delivery purposes. Correctly configured MX records are essential for successful mail flow within organizations hosting their own e-mail servers. For example, you may have an e-mail server on your network with the name email1.contoso.com which hosts all e-mail accounts for the domain contoso.com. You would need to create a MX record to map the domain name contoso.com to email1.contoso.com. This record tells other e-mail servers on the Internet which e-mail server to connect to when trying to deliver e-mail messages to contoso.com. Without an MX record all e-mail messages would have to be addressed

to the host record itself. All contoso.com e-mail addresses would appear as username@email1.contoso.com instead of username@contoso.com. MX records can also be used to provide redundancy to your messaging system. Each MX record has an associated “cost.” For example, let’s assume you have two e-mail servers on your network. These servers are named email1.contoso.com and email2.contoso.com. Email1 is the primary server responsible for message delivery. You want email2 to take over e-mail delivery if email1 is unavailable. To achieve this you would need to setup two MX records. The first MX record would map contoso.com to email1.contoso.com and have a cost set to 5. The second MX record would map contoso.com to email2.contoso.com and have a cost set to 10. Since 5 is the lowest cost all e-mail for contoso.com will be delivered to this server as long as it is online. However if email1.contoso.com goes offline email2.contoso.com would begin receiving all e-mail for contoso.com.

- **NS (Name Server) Record** NS records identify all authoritative DNS servers for a zone. These records are crucial when you have multiple DNS servers set up for redundancy.
- **SRV (Service) Record** SRV records are used to provide auto-discovery of TCP/IP resources on a network. SRV records allow clients to simply query the domain for information regarding which server or servers they should connect to for a particular service. For example, when you install Active Directory on your network, several SRV records are created for Kerberos. A workstation may need to find a domain controller to obtain a Kerberos ticket. The workstation can simply query DNS for a list of those servers offering Kerberos services, in this case your domain controllers.
- **PTR (Pointer) Record** PTR Records complete the exact opposite task of A records. PTR records map an IP address to a host name. By using PTR records you can find a host name by simply knowing the IP address. For example you may know a server’s IP address is 10.4.2.3. By querying DNS you can find out that 10.4.2.3 is a server named web3.syngress.com. PTR records are stored reverse lookup zones mentioned earlier in this section.

DNS can be installed by the Add Role wizard like any other role. DNS can also be automatically added when you add the active directory role. Many services on a Windows network rely on a working and healthy DNS deployment to function properly. As a network administrator you should properly plan for a highly available and redundant DNS deployment in your organization.

## Planning for Dynamic DNS (DDNS)

Microsoft has provided Dynamic DNS (DDNS) capabilities since the release of Windows 2000. DDNS allows authorized hosts or servers to automatically update records within DNS. Without DDNS you would need to manually update the DNS record for computers when their IP addresses changed. As you can imagine, the administrative overhead of doing this would be unmanageable in most networks, especially those with a lot of laptop computers that constantly get a new IP address. DDNS capable zones can also be configured to allow DHCP clients to update their own host records. One of the following DDNS options must be configured for all Windows Server 2008 hosted DNS Zones:

- **No** This option does not allow dynamic updates and all records must be manually managed and updated.
- **Yes** All dynamic update requests.
- **Secure Only** This option is only available for Active Directory integrated zones and provides a higher level of security for dynamic updates.

### *Scavenging*

Dynamic DNS provides a great way to automatically create and update DNS records for hosts on your network. This feature, however, also causes DNS to host stale or outdated records. For example, you may temporarily add a test workstation to your network. The workstation can perform a dynamic update with DNS and create an A record for itself. What happens when you decide to turn off that test computer to never be used again? The DNS record remains until it is manually deleted. As you can see this could cause DNS to become polluted with hundreds or thousands of unused records on even a medium sized network. Scavenging addresses this problem by periodically removing outdated records. When dynamic records are created they are given a timestamp. You can configure scavenging to automatically delete old, unused records based upon this timestamp field. This timestamp can be updated when hosts or DHCP perform updates on records. Scavenging can be used to periodically delete records whose timestamp have not been updated or has become stale.

## Planning For DNS Forwarding

You should consider forwarding as part of your DNS deployment. This allows you to configure a designated DNS server as a forwarder. Other DNS servers will send requests to this server when they cannot resolve a query. For example, you may have a DNS server setup with a zone named contoso.com. This DNS server

is authoritative and will perform all name resolution requests it receives for the contoso.com domain. However if a DNS query is made to this same server for syngress.com, it needs a way to forward this request on to another DNS server. By default forwarding takes place by the use of root hints. Root hints are by default configured as the Internet root DNS servers. Root hints are automatically configured when the DNS role is added to a Windows Server 2008 computer. For security and management purposes you may decide to manually set up forwarding. When manually configuring forwarding you instruct the DNS server to send any requests that it can't resolve to another DNS server of your choice rather than using root hints. This configuration can be done at the server level or by conditional forwarding. Server level forwarding will forward any request that the DNS server cannot resolve to another server specified in the forwarding configuration. Conditional forwarding will only forward requests for specified DNS domain names. Many organizations use DNS forwarding to configure their network so that the internal corporate DNS servers never perform queries for Internet-based domains. For example, you may want to set up a group of DNS servers in your DMZ or perimeter network. You could configure those DNS servers to use root hints to resolve all queries. You could then configure your internal DNS servers to forward requests to the DMZ servers. This method can provide an extra layer of security for your DNS infrastructure.

Planning for your DNS deployment is essential to ensure you have a well-organized and reliable infrastructure. Many mission-critical services and applications rely on DNS, which makes it one of the most critical components of your Windows network.

## Network Access Protection

Windows Server 2008 delivers a new feature to ensure client computers connecting to your network comply with IT health policies. Network Access Protection (NAP) makes sure that client computers have current operating system updates installed, antivirus software running, and other configurations set up related to ensuring the client is compliant with IT health policies. NAP can also be integrated with third parties to create even more sophisticated health policies for your Windows clients. Before deploying NAP you must carefully consider how and where you will use the technology. This section will discuss planning your NAP deployment.

### Planning for NAP Enforcement Methods

When deploying NAP, you must consider what enforcement methods you need. The methods you use will rely heavily on what technologies you have deployed or

will deploy on your network. For example, you can't enforce NAP on a Terminal Services Gateway, if you don't deploy a Terminal Services Gateway. The following enforcement methods are available for NAP:

- **DHCP** DHCP can be used to only provide a subset of the IP configuration during a DHCP request or renew. This configuration allows the client to become compliant before it is issued the full IP configuration.
- **IPsec** Ensures the client is health compliant before issuing a certificate which is needed to communicate with other computers on the network.
- **802.1x network switches** 802.1x compliant switches can be used to VLAN unhealthy systems to a remediation VLAN. After the system is compliant with health policies it is then reassigned to the production VLAN.
- **VPN** NAP can check the health of the client before allowing the computer to complete a VPN connection into the corporate network.
- **Terminal Services Gateway** NAP can be used to ensure only health compliant computers are allowed to access the corporate network via a Terminal Services Gateway.

Any of the above enforcement methods can be used to enforce NAP. You could also use a combination of any of the above enforcement methods. For example, you could deploy both DHCP-based enforcement and Terminal Services Gateway deployments. Let's discuss the above enforcement methods a little more in detail and when to use them.

## Configuring & Implementing...

### Planning for Network Access Protection

Network Access Protection (NAP) deployment requires ensuring both servers and physical networks are properly configured. If you do not manage your network switches and routers, you may need to involve the team that does. This is especially true if you plan to deploy 802.1x or VPN-based NAP.

## Planning For DHCP NAP Enforcement

Using DHCP enforcement is the quickest and easiest method to set up and configure. DHCP enforcement begins by providing the client with only a base IP address with no gateway configuration. Once the computer has been validated as “healthy” it is provided a full access IP address. DHCP-based enforcement only requires that you set up the DHCP and NAP server roles. These roles can reside on separate servers or the same one. DHCP NAP enforcement may not meet the security requirements of some organizations because anyone with administrative access to his computer can override NAP by simply assigning a static IP address.

## Planning For IPSec NAP Enforcement

IPSec enforcement is considered the most secure form on NAP because it can be used to limit communications based on IP addresses and port numbers. Unlike DHCP enforcement, IPSec enforcement does not begin until after the computer has obtained a valid IP address. Using IPSec Rules, computers must first be validated as “healthy” before other compliant computers will accept network packets from them. This validation is performed by ensuring the client is compliant with the required health policies. If the computer is deemed compliant it is given a health certificate which allows it to communicate with other validated computers. An IPSec-based deployment is set up with three logical network layers.

- **Restricted Network** An outer restricted network is where clients are initially placed when physically connecting to the network. Computers can only talk to a middle layer boundary network for health remediation.
- **Boundary Network** The middle layer network contains only remediation servers to allow unhealthy computers to become healthy so that they can become part of the secure network.
- **Secure Network** This inner network layer contains only computers that have passed health validation and have a health certificate. Computers in this layer can speak to other computers in the secure network as well as computers in the boundary network.

IPSec is a very secure form of NAP enforcement. When planning to deploy IPSec Enforcement you will need to plan to deploy a Public Key Infrastructure (PKI) if you haven’t already done so. IPSec Enforcement relies heavily on the use of certificates.

## Planning For 802.1x NAP Enforcement

802.1x enforcement requires that network devices such as switches or wireless access points support the 802.1x technology. This is a standards-based protocol that most newer network equipment will support. If your network switches do not support this protocol, you may not be able to use this method to provide NAP enforcement. Using 802.1x allows you to easily set up a remediation Virtual LAN (VLAN). This allows you to physically ensure unhealthy computers cannot talk to computers except remediation servers until it passes the health validation process. The 802.1x method works like this:

1. A client connects to the physical network.
2. The network switch or access point authenticates the computer by using a RADIUS Server.
3. The health of the computer is validated.
4. If the computer is noncompliant with the health policies, the 802.1x switch will place the computer on an isolated VLAN for remediation.
5. After remediation is complete and the computer passes health validation, the 802.1x network device will allow the computer to communicate on the normal secure network.

802.1x enforcement allows you to control network access and validate the health of computers by using 802.1x compliant network switches and wireless access points. You should carefully review your network topology before deploying 802.1x as you may need to configure remediation VLANs. If your switches and access points do support 802.1x you may want to consider this option for deploying Network Access Protection.

## Planning For VPN NAP Enforcement

The VPN NAP enforcement method allows you to ensure remote computers connecting to your network via VPN are compliant with health policies. If a computer connecting via VPN is noncompliant, it is provided limited network access by the use of packet filters. VPN NAP will also periodically check the health of the

remote computer. If it falls out of compliance then it will be restricted using the same packet filter method. You may want to consider using VPN NAP enforcement if you provide or plan on providing VPN access to your network.

## Planning for NAP Servers

When planning to set up NAP on your network you must plan to deploy the proper servers to support NAP. Your NAP infrastructure must at the very least include Health Policy Servers (NPS) and Health Requirement Servers.

If you choose to deploy IPSec-based NAP you will also need to deploy Health Registration Authority Servers. You also will want to ensure you have remediation servers set up on the restricted network to help noncompliant systems become compliant. Thought not mentioned in this section, you must deploy required enforcement servers for the enforcement method you choose. For example, you can't deploy DHCP enforcement without deploying a DHCP Server.

### *Health Policy Servers*

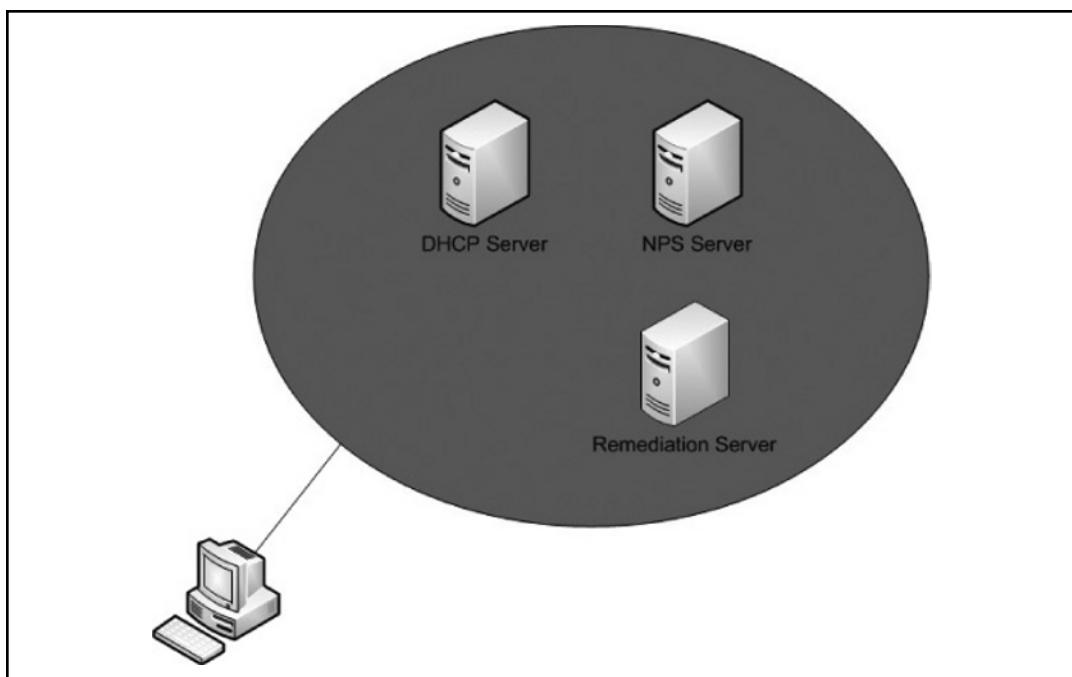
Health Policy Servers provide the core functionality of NAP. The NPS role is installed on these servers. Health Policy Servers store health policies that you define and validate client health compliance. The Health Policy Servers then work with the enforcement methods previously discussed in this chapter to either grant full network access or provide the client access to only remediation servers.

### *Health Requirement Servers*

Health Requirement Servers maintain data that Health Policy Servers use to determine if a client is compliant with health policies. Health Requirement Servers store information such as update information and antivirus definitions.

### *Health Registration Authority Servers*

Health Registration Authority (HRA) Servers are used when deploying IPSec-based enforcement. HRA Servers provide certificate services and offer health validation certificates to NAP clients. HRA Servers are also the enforcement point for IPSec-based NAP. Figure 1.17 depicts a typical NAP deployment using DHCP enforcement.

**Figure 1.17** DHCP Enforced NAP Deployment

## Planning for NAP Clients

Before deploying NAP you need to take your current client versions into consideration. Windows Server 2008 NAP supports only Windows Vista, Windows Server 2008, and Windows XP Service Pack 3 clients. Support for other client operating systems such as Linux and Mac OS may be provided by Microsoft ISV partners.

## Directory Services

Before deploying directory services you should understand their purpose and what features they provide to Windows networks. The best example of a directory service is a phone book. Phone books hold names and their associated properties such as phone number and address. Directory services on corporate networks provide similar functions. Network directory services can store and manage network objects such as computers, users, and printers as well as their associated properties. Directory services provides a single location to manage and search for network objects. Microsoft first introduced its version of directory services late in the life of Windows NT 4.0. However the first true directory service for Windows

networks, Active Directory, was introduced with the release of Windows 2000 Server. Depending on the type of Windows network you are deploying, planning your Active Directory deployment could be the single most critical step of the planning process. The health of your entire Windows network will probably be dependent on this service. Active Directory is the service for hosting user accounts, security settings, network segment information, and even the configuration information for the Windows domain. Other Microsoft products that you may deploy rely heavily on Active Directory. The foremost of these is Microsoft Exchange server. Exchange server uses Active Directory for mailbox information and even mail routing. Fortunately Microsoft has put a lot of development effort into ensuring Active Directory is a stable and reliable directory service.

You may already have Active Directory deployed in your existing Windows 2000 or Windows 2003 network. If this is the case there are upgrade choices you must consider. In this section we will cover planning for a fresh deployment of Active Directory as most of the concepts still apply if simply upgrading your deployment.

Let's start by taking a look at planning a fresh Active Directory deployment. You must consider things such as the operating system of your workstations, security and administrative boundaries in your organization, WAN links, number of users, and applications that may rely on Active Directory.

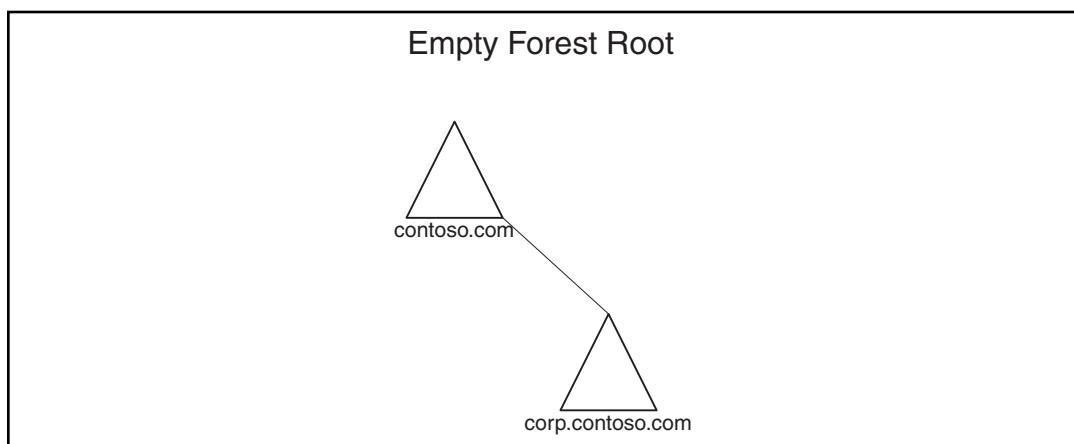
## Planning Forests and Domains

When planning your Active Directory deployment, one of the first decisions you should consider is how many Forests and Domains to deploy. To properly plan Forests and Domains you need a clear understanding of some key Active Directory terms. Be sure you know the following:

- **Domains** A domain is the foundation of Active Directory. Domains contain objects such as users, computers, and printers. One or more domains make up Active Directory.
- **Trees** A tree is composed of one or more domains arranged in a hierarchical fashion. Trees are made up of a parent domain and one or more child domains. The child domains use a name appended to the DNS name of the parent. For example, you may have a parent domain named contoso.com and a child domain named northamerica.contoso.com. The two domains makeup a tree. Child domains must always inherit the fully qualified domain name of the parent. Trees are a great way to provide a central security model but delegate rights to other domains within the tree.

- **Forests** A forest is a collection of one or more trees. Forests use different fully qualified domain names (FQDN). Forests maintain independent security but allow interaction between all domains in the organization. All domains in a forest have a two-way transitive trust.
- **Organizational Units (OU)** Organizational Units are containers for domain objects such as user accounts or computers. OUs allow you to organize domain objects for ease of management. You can almost think of OUs as a folder. Instead of organizing files, you are organizing domain objects.
- **Sites** Active Directory Sites are one or more connected IP subnets. Microsoft defines a site as a subnet or group of subnets in which all devices are connected via a fast and reliable connection.

In some situations due to security or ownership requirements it may be necessary to deploy multiple domains or forests. For example you may acquire a company that already has an existing Active Directory forest. You may need to maintain that existing forest instead of migrating those users into your existing Active Directory forest(s). Determining the number of domains or forests to create can be one of the toughest and most critical decisions you make when deploying Active Directory. You may want to deploy multiple domains or forests if you require a decentralized administration model, have different regulatory requirements, or want to take advantage of resource domains. Some organizations are using resource domains to host server applications such as Microsoft Exchange Server. By using a separate resource domain you can ensure separation of duties for Exchange and Active Directory Administrators. Some organizations choose to deploy a root forest that only hosts the enterprise administrator accounts. They will then deploy a child domain that hosts all computers, users, and applications. This provides an additional layer of security (and complexity) to your Active Directory deployment. Be sure to consider all aspects and repercussions when planning your forest and domain design for Active Directory. Figure 1.18 shows an example of an empty forest root deployment. The contoso.com domain would only be used for administrative purposes while the child domain (corp.contoso.com) contains all resources such as computers and standard user accounts.

**Figure 1.18** Empty Forest Root Active Directory Deployment

## Planning Domain Controller Placement

When deploying domain controllers you must determine where they should be located and how many to deploy. For example you may want multiple domain controllers in larger offices for redundancy. This would prevent computers from authenticating over the WAN in the event of a single domain controller failing within a site. In smaller offices with few users, it may be acceptable for them to authenticate with domain controllers over the WAN. Another planning consideration you must think about is physical security of the location in which the domain controller will reside. For example, placing a domain controller under the receptionist's desk is a bad idea. Remember Active Directory, which includes users, passwords, and other security configurations, is stored on that DC. Be sure you can provide physical security to a domain controller before placing it in a location. You also may want to consider using a server core install for some of your domain controllers. If you remember, server core only installs essential software to support the infrastructure services you define. Active Directory is one of the services offered in a server core install. Using server core for domain controllers provides not only a reduced attack surface but also a greater level of protection from the average end user or inexperienced administrator. Since server core does not include a GUI interface, you must know how to use the operating system command line or use administrative tools connected to the server remotely.

## New & Noteworthy...

### Planning for Read-Only Domain Controllers

Windows Server 2008 introduces Read-Only Domain Controllers (RODCs). RODCs provide a greater level of security for branch office or remote domain controllers. RODCs can never make updates to Active Directory. RODCs also only provide credentials for users in the same site as that DC and never stores any administrator credentials. This provides a much greater level of security for Domain Controllers (DCs) that may be placed in locations with little or no physical security. For example, you may have a DC located in an unsecure closet in a small branch office. Though this is not an ideal location for a DC it is sometimes reality. If someone steals this DC you can easily see what credentials were stored on that DC and reset the password for the employees in that branch only. You can also rest assured that your domain admin account credentials were not stored on that DC.

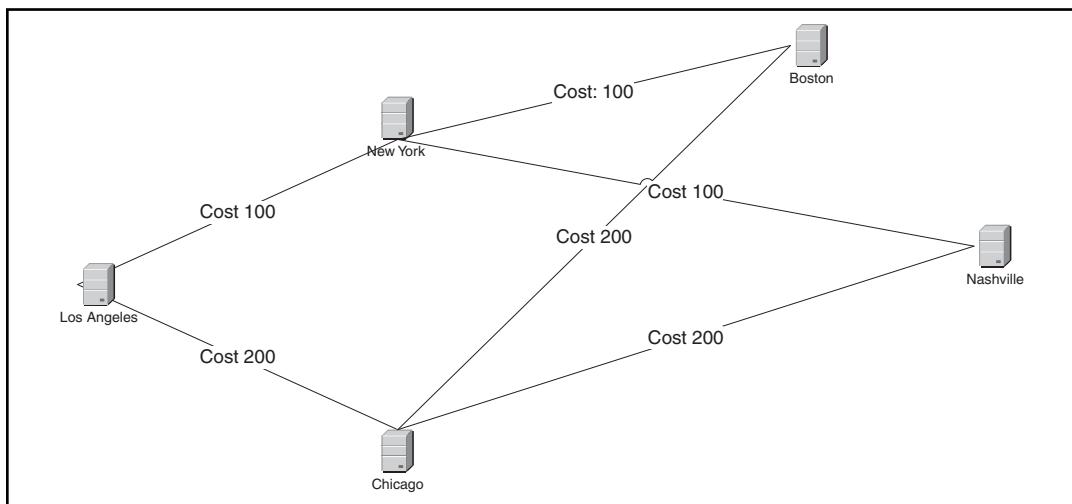
## Planning Active Directory Sites and Site Links

When planning your Active Directory deployment, site planning should be considered to ensure reliable and consistent logon services are offered to your workstations as well as efficient Active Directory replication. Proper site planning is also crucial to ensure your WAN links are not saturated with log-on traffic. If you are deploying Active Directory in an organization without a Wide Area Network (WAN), then site planning is a quick and painless process. However if you have multiple locations connected over a WAN, you must properly plan for Active Directory sites.

Microsoft defines an Active Directory site as any network where all systems are connected by a 10 MB or greater link. An example of this would be the local LAN in an office. Sites are defined by the use of IP subnets. Computers determine which Active Directory site they are located in by which subnet their IP address resides in. This allows computers to first send an authentication request to a domain controller in the same site before sending the request over the WAN to a domain controller in

a different physical location. The use of Active Directory sites also determine how often domain controllers replicate with each other. A copy of the Active Directory database is stored on each domain controller and can be updated on every domain controller in which it is stored (with the exception of Read-Only Domain Controllers). To ensure the database is consistent Active Directory must replicate the database to all domain controllers. The Knowledge Consistency Checker (KCC) will automatically create replication connections for domain controllers within a site. The KCC will also automatically create replication connections for domain controller between sites after site links are created. How often this replication occurs is partially controlled by Active Directory sites. Domain controllers within a site automatically replicate every 5 minutes. This is called intra-site replication. However replication times between domain controllers in separate sites can be configured using the Active Directory sites and services console. Replication between sites is called Inter-Site replication. You may want to limit replication between sites to occur on a less frequent basis to prevent excessive use of bandwidth on slow WAN links. However you should keep in mind that long periods without replication means changes to active directory objects take longer to fully replicate to all other domain controllers. For example, you receive a call that a new employee is starting this morning in your New York office. You create the new user account on a domain controller in the Detroit office. If the Detroit site does not replicate with the New York site but once per day, then that user account may not be available in the New York office until tomorrow morning. Keep these types of situations in mind when planning site replication for Active Directory.

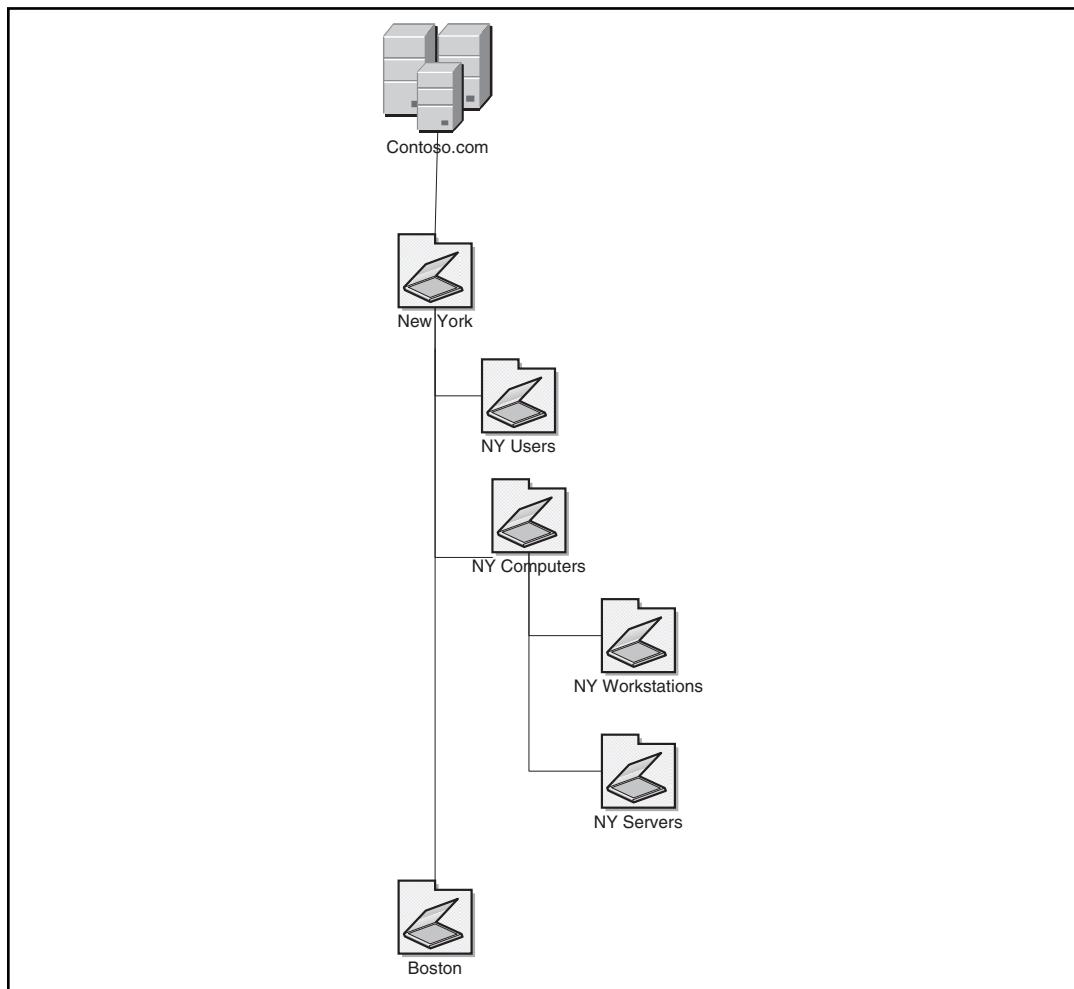
Another aspect of planning your site deployment is the use of site links. Site links are the mechanism that Active Directory uses to replicate between sites. Each site can have one or multiple site links configured to replicate with other sites. When possible you should consider configuring multiple site links between sites. This allows Active Directory replication to continue in the event of another site failing. This can be achieved by configuring the cost of each site link. For example a site link between the Boston Office and the New York office could have a cost of 100. The link between Boston and Chicago has a cost of 200. As long as the link between Boston and New York is available it will use this link to replicate since the cost is lower. However if the link between Boston and New York is unavailable, replication will fail-over to the link between Boston and Chicago. Figure 1.19 depicts a typical hub and spoke replication scheme with a redundant hub site. Figure 1.19 depicts a medium-sized organization's site and replication topology.

**Figure 1.19 Active Directory Replication Topology****EXAM WARNING**

! Don't get tripped up by site link costs. Be ready for several questions related to Active Directory replication within a site (Intra-Site Replication) and between sites (Inter-Site Replication). Also be sure to fully understand site link costs and how their weight determines which sites the KCC will generate replication.

## Planning Organizational Unit Design

You should plan for the Organizational Unit structure of your domain when planning your Directory Services deployment. OU design can be based on geography, organizational structure, administrative boundaries, or just about any other structure you can think of. When planning your OU design you should carefully consider how the OUs will be used when delegating permissions or managing objects within the OU. As a rule of thumb, every OU should have a well defined use. For example you could create an OU for every location in your company; however, one location might only house three users with three computers. Unless there is a need to manage those three computers or users independently you would not want to create a separate OU for them. If you ever have an empty OU, then chances are you don't need it. Don't add complexity to your environment if it doesn't help you solve a problem. See Figure 1.20 for an example of good OU design based on geographic location.

**Figure 1.20** Organizational Units

### *Delegating Authority to Organizational Units*

One of the key benefits of using Active Directory Organizational Units (OUs) is to provide the ability to delegate the ability to change items within those OUs.

By delegating control you can give other users the ability to make changes to objects only within OUs in which they have been given permission without elevating their overall permissions. Keep this feature in mind when designing your OU structure.

## EXERCISE 1.3

### DELEGATING PERMISSIONS TO AN ORGANIZATIONAL UNIT

1. Open Server Manager by clicking Start | Administrative Tools | Server Manager.
2. Expand the nodes Roles | Active Directory Domain Services | Active Directory Users and Computers | *YourDomainName*.
3. Create a new Organization Unit (OU) by right clicking the domain name and choosing New | Organizational Unit. This will launch the New OU Wizard.
4. Enter the name **Boston** and click the OK button.
5. You will now see a new Boston OU as seen in Figure 1.21.

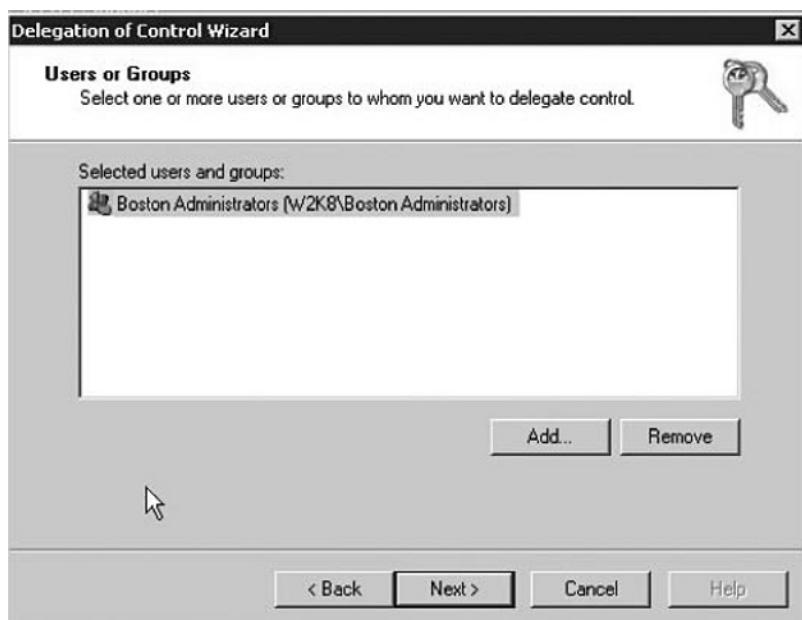
**Figure 1.21** Boston Organizational Unit



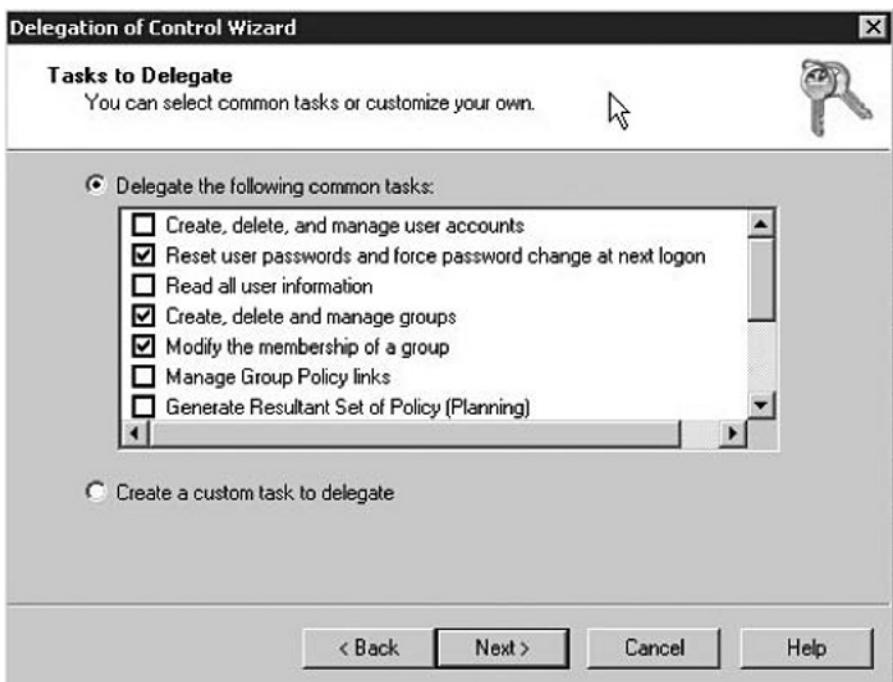
6. Right-click the **Boston** OU and select **Delegate Control**. This will launch the **Delegation of Control Wizard**. Click the **Next** button to continue.
7. We now have to decide who we want to delegate permissions to. This is the users or groups we want to provide a higher level of rights for objects contained in this OU. In our example we will be

adding a group named **Boston Administrators**. Click the **Add** button to locate the **Boston Administrators** group (See Figure 1.22). Then click the **Next** button.

**Figure 1.22** Select Users or Groups



8. We now need to configure what permissions to give the **Boston Administrators**. In our example we want to provide the Boston Administrators group with the ability to reset user passwords and create and manage groups and their memberships. Go ahead and select the options **Reset user passwords** and **force password change at next logon**, **Create delete and manage groups**, and **Modify the membership of a group** (See Figure 1.23). Then click the **Next** button.

**Figure 1.23** Selecting Permissions for the Boston OU

9. Click the **Finish** button to complete the wizard.

You have successfully provided the Boston Administrators group with permissions to reset passwords and manage groups, but only within the Boston OU. To provide any user the ability to manage passwords and groups in the Boston OU, simply add them to the Boston Administrators group.

## Planning for Automated Server Deployment

Many organizations are faced with deploying hundreds or even thousands of servers. This task can become very time consuming even for smaller IT department. This is especially true when installing additional software and services such as antivirus and backup agents. Complete setup of a server from bare-metal to fully deployed can take hours or even days. Many organizations have helped speed deployment time by using imaging programs such as Symantec Ghost or Microsoft's own deployment tools Remote Installation Services (RIS) for workstations and Automated Deployment Services (ADS) for servers. With the release of Windows

Vista and Windows Server 2008, Microsoft has incorporated the two services into one. This new service is Windows Deployment Services (WDS). WDS allows you to easily create standard server installations or images and rapidly deploy them across your organization. When planning your Windows Server 2008 deployment you should consider the use of WDS to ensure all servers use a standard configuration and that you can rapidly install new servers. In this section we will cover how to plan and setup WDS as well as create standard server images which can be rapidly deployed and even deployed at a scheduled time.

There are several considerations you must take into account when setting up WDS. WDS requires proper infrastructure components that it depends on already be deployed. Before using WDS you must ensure the following are setup and configured properly on your network.

- **Active Directory Domain** The WDS Server must be a member of an existing Active Directory Domain, covered later in this chapter.
- **DNS** WDS requires DNS be properly configured
- **DHCP** In order for WDS to function properly a Dynamic Host Configuration Protocol (DHCP) service must be available on your network.
- **PXE boot capable Server** Servers that you wish to use WDS to deploy the operating system to, should support PreBoot Execution Environment (PXE). PXE is the process of booting a computer from its network adapter. Typically this process involves pulling a boot image down from the network and loading into the computer's memory. This feature is available on most enterprise servers today.

Information on setting up the above services can be found later in this chapter. For now we will assume the above services are available on your network. Let's walk through setting up and configuring Windows Deployment Services.

## EXERCISE 1.4

---

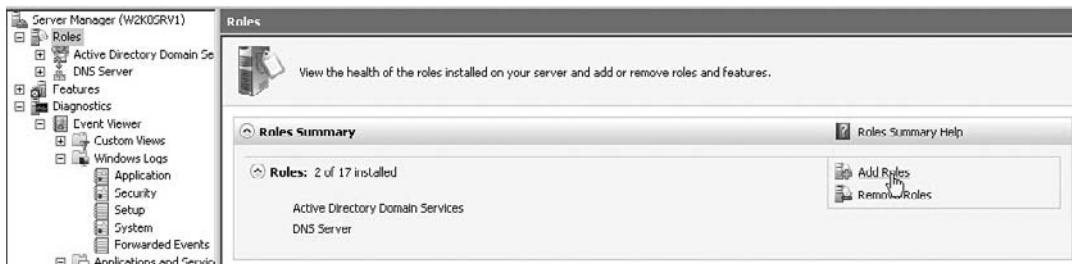
### INSTALLING AND CONFIGURING WINDOWS DEPLOYMENT SERVICES

After you have made sure the prerequisites for Windows Deployment Service have been met, we can set up and configure WDS.

1. Open **Server Manager** by going to **Start | Administrative Tools| Server Manager**.

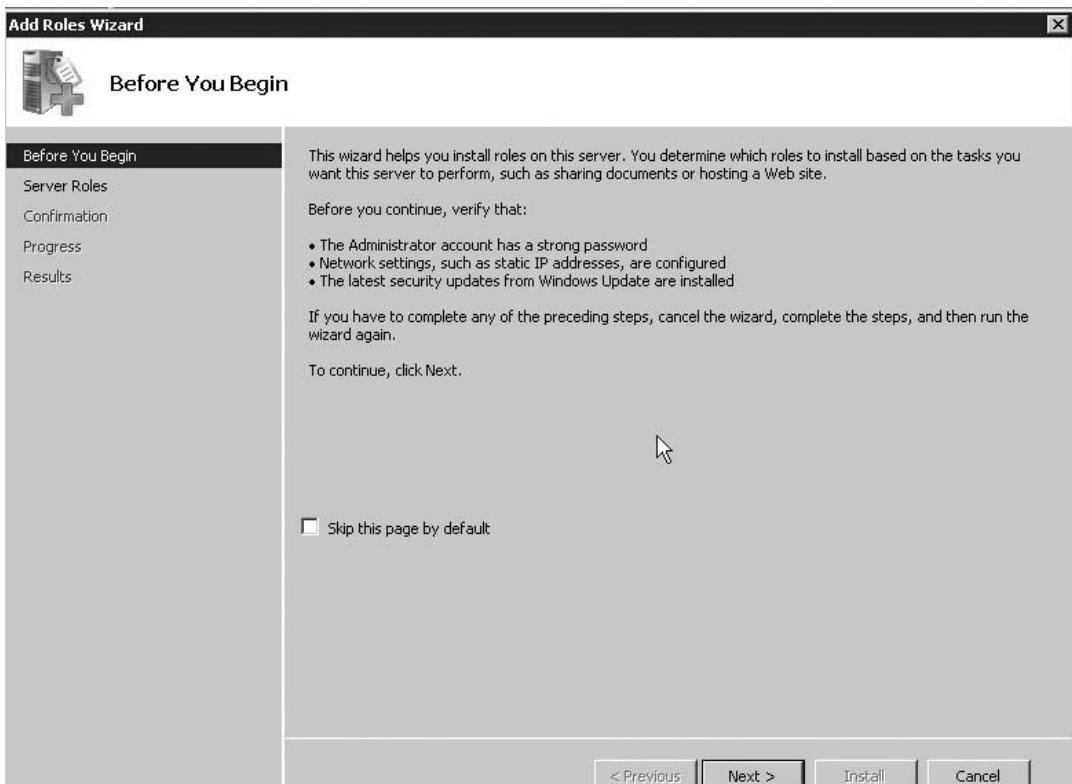
2. From the **Roles** section, as seen in Figure 1.24, click the **Add Roles** link.

**Figure 1.24** Server Manager



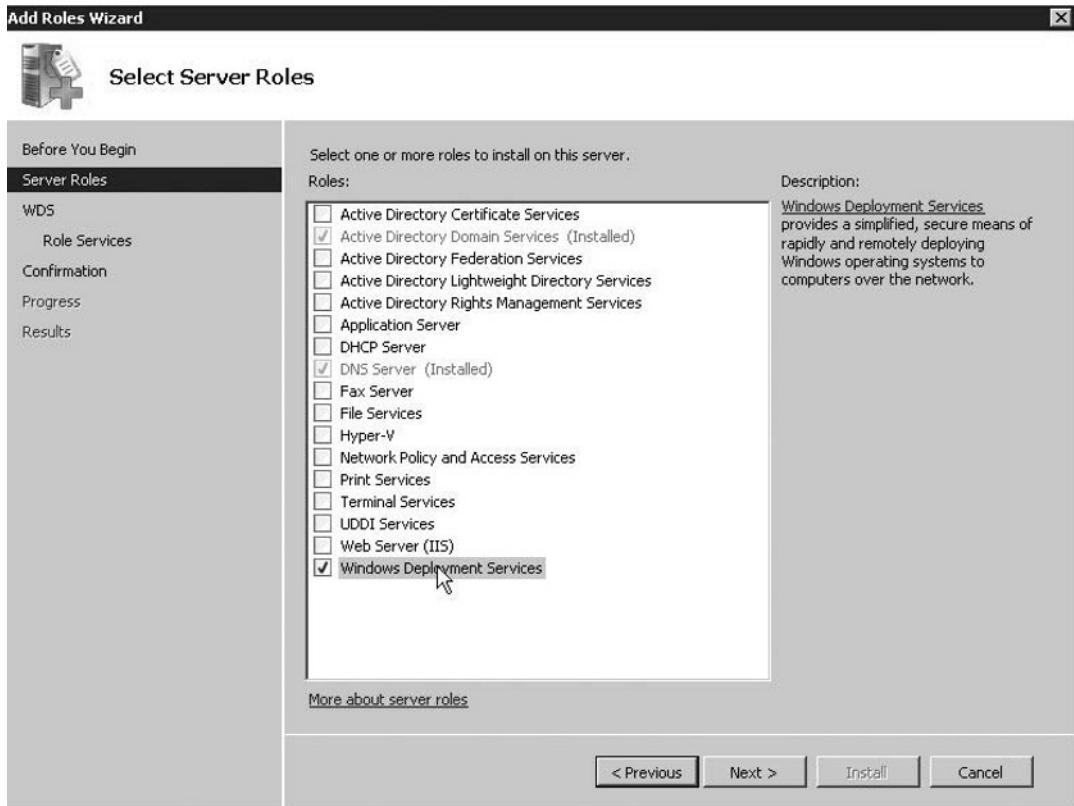
3. The **Add Roles Wizard** will launch as seen in Figure 1.25. Click **Next** to continue.

**Figure 1.25** Add Roles Wizard

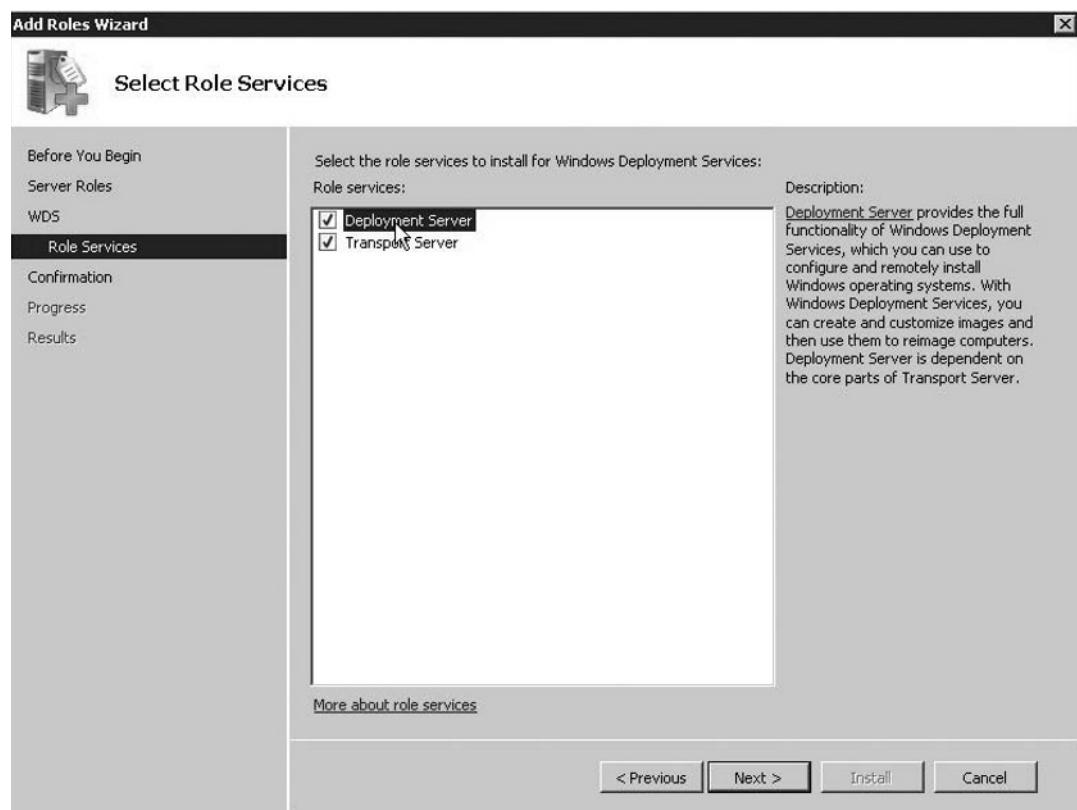


4. Select **Windows Deployment Services** from the list of available roles (See Figure 1.26). Then click the **Next** button.

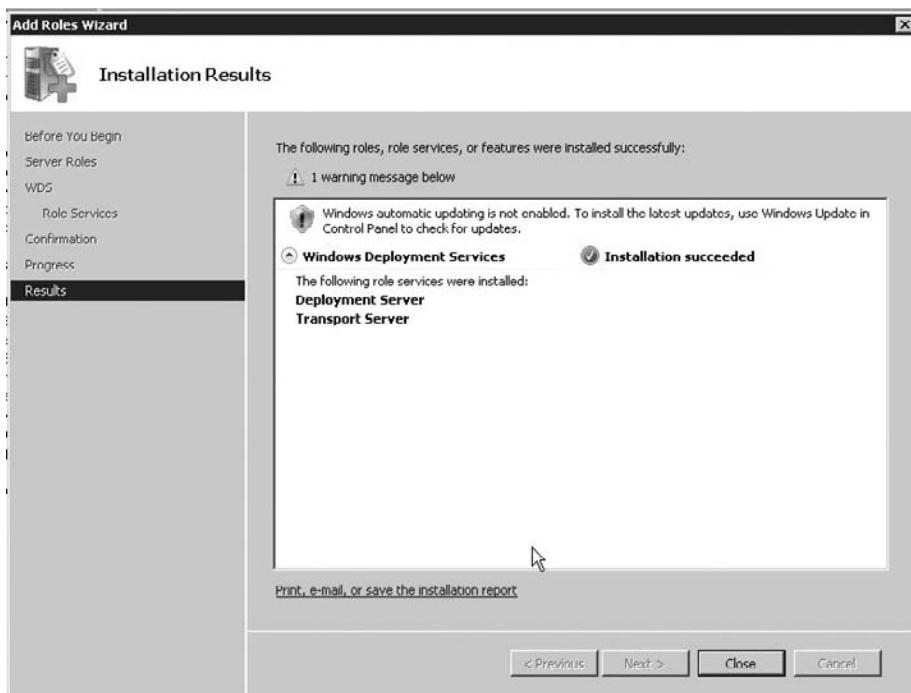
**Figure 1.26** Select WDS Server Role



5. On the **Summary** page of the wizard click the **Next** button.
6. Make sure the **Deployment Server** and **Transport Server** are selected on the **Role Services** page as seen in Figure 1.27. Then click the **Next** button.

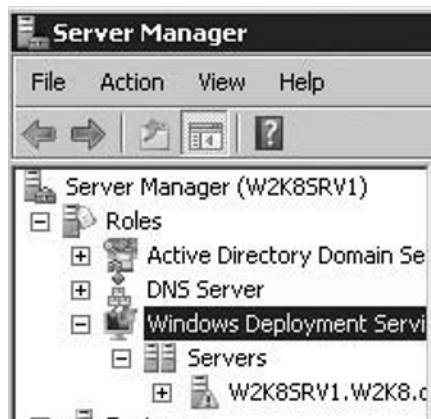
**Figure 1.27 Select Role Services**

7. Confirm your selections on the summary screen then click the **Install** button. This will install the necessary files to run WDS on this server. You should see a summary page indicating the install was completed successfully after completion (See Figure 1.28). Click the **Finish** button.

**Figure 1.28** WDS Install Successful

Now that we have successfully installed Windows Deployment Services, we need to configure the service. You should now see the Windows Deployment Services node within Server Manager.

8. Expand the **Windows Deployment Services | Servers** node in **Server Manager**. Locate the name of your server as seen in Figure 1.29.

**Figure 1.29** Windows Deployment Services in Server Manager

9. Right-click the server and choose **Configure Server** from the menu (see Figure 1.30)

**Figure 1.30** Windows Deployment Services—Configure Server



10. The **WDS Configuration Wizard** will launch and a summary page will be displayed, as seen in Figure 1.31. Again verify you have met the prerequisites listed on this page. Then click **Next** to continue.

**Figure 1.31** Windows Deployment Services Configuration Wizard

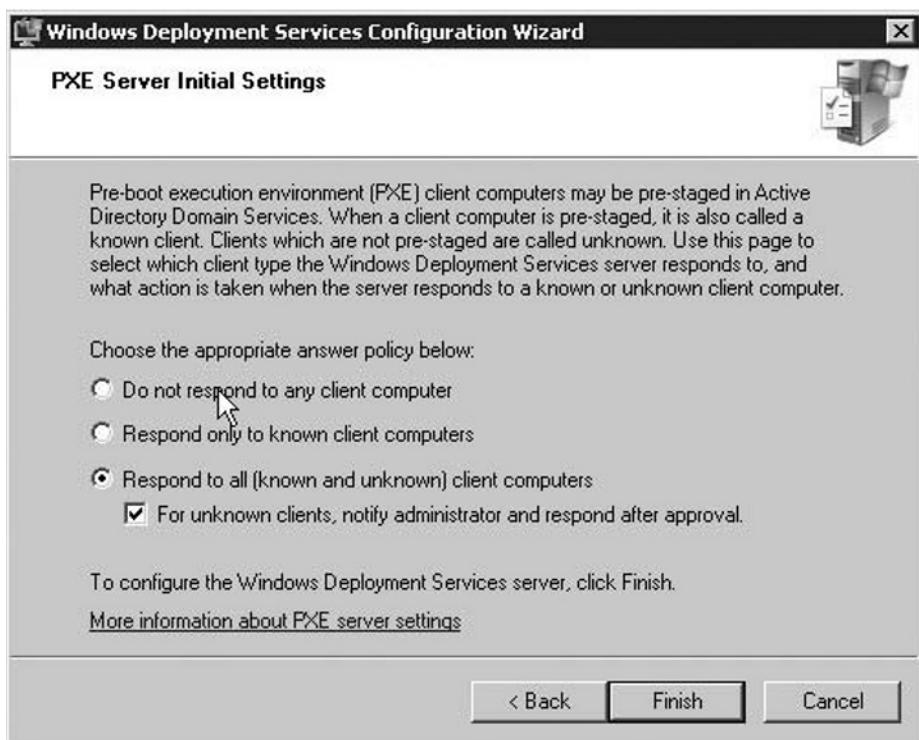


11. Choose the location you wish to store the images to be deployed via WDS (See Figure 1.32). You should ensure this location is large enough to store large files. Microsoft does not recommend using the same drive as the operating system to store images.

**Figure 1.32** Remote Installation Location



12. You now must select how you want WDS to respond to PXE clients. In our example let's choose the option to **Respond to All Known and Unknown client computers** and **Notify the Administrator** (See Figure 1.33). Then click **Next**.

**Figure 1.33** PXE Configuration

13. You can go ahead and add images from a Windows Server 2008 DVD at this time if you wish. Go ahead and select the option to **Add Images to the Windows Deployment Services Server now**. Then click the **Finish** button.
14. Enter the location of the WDS images (See Figure 1.34), for example your Windows Server 2008 DVD, then click **Next**.

**Figure 1.34** Source Image Location



15. Go ahead and create a new image group. Image groups allow you to logically organize your WDS images for ease of management. Enter the name of your new image group and then click **Next**.
16. Review the settings and then click **Next**. This will add the OS images to your WDS deployment. It may take several minutes to add the images to WDS. After the addition is complete you should now see the images and your new image group under the WDS Server in **Server Manager** as seen in Figure 1.35.

**Figure 1.35** OS images

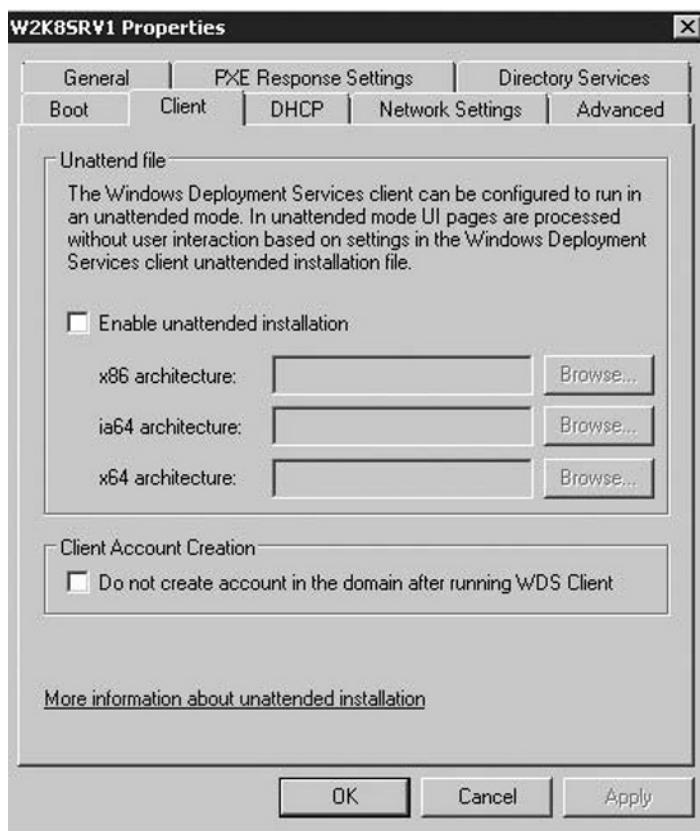
The screenshot shows the 'Server Manager' interface. On the left, the navigation pane includes 'File', 'Action', 'View', 'Help', and icons for 'File Explorer', 'Task List', and 'Search'. Under 'W2K8 SRV1', there are sections for 'Active Directory Domain Services', 'DNS Server', 'Windows Deployment Services' (which is expanded to show 'Servers', 'Install Images' (with 'W2K8 DVD' selected), 'Boot Images', 'Legacy Images', 'Pending Device', and 'Multicast Trans'), 'Features', 'Diagnostics', 'Configuration', and 'Storage'. The central pane displays a table titled 'W2K8 DVD Images' with the following data:

Image Name	Architecture	Status	Size	Date
Windows Longhorn SERVERENTERPRISE	x64	Online	838...	1/19...
Windows Longhorn SERVERDATACENTER	x64	Online	820...	1/19...
Windows Longhorn SERVERSTANDARD	x64	Online	239...	1/19...
Windows Longhorn SERVERENTERPRISECORE	x64	Online	240...	1/19...
Windows Longhorn SERVERDATACENTERCORE	x64	Online	240...	1/19...
Windows Longhorn SERVERSTANDARD	x64	Online	838...	1/19...

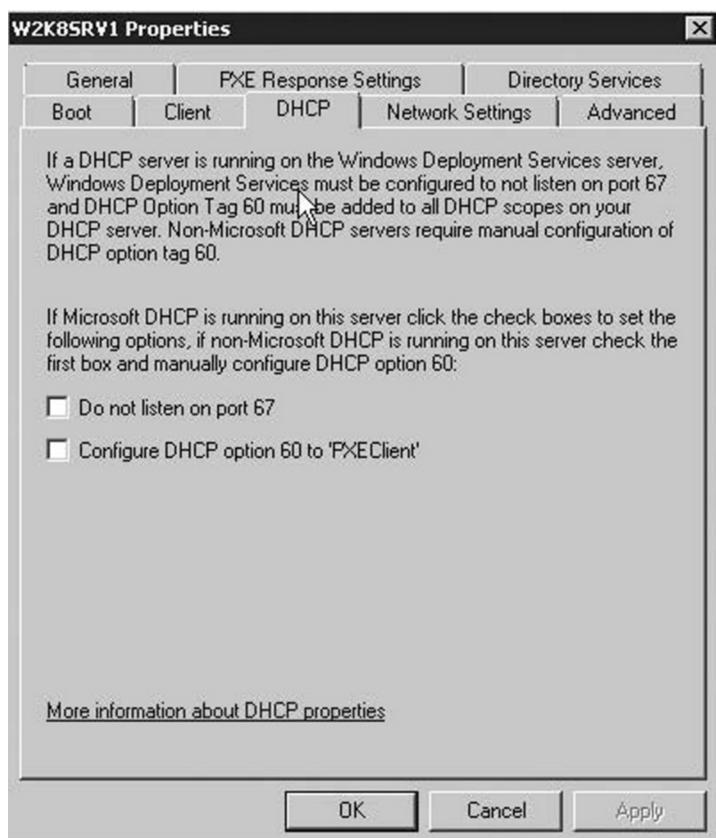
On the right, there is an 'Actions' pane with a 'More Actions' dropdown menu.

17. You should also see a boot image under the **Boot Images** node. This is the image used to PXE boot computers attaching to WDS.
18. Let's go ahead and look at a few more options for WDS. Right-click on the WDS Server and choose **Properties** from the pop-up menu.
19. The **Properties** window will be displayed. Go ahead and click the **Client** tab. On this tab you can add unattended installation scripts to auto choose the install options when installing an OS image (See Figure 1.36).

**Figure 1.36** WDS Properties—Client Tab



20. Go ahead and click the **DHCP** tab. On this tab you can select two options necessary if you installed WDS on the same server that also hosts the DHCP role. If this is the case you must select two options, **Do not listen on port 67** and **Configure DHCP option 60 on 'PXEClient'** (See Figure 1.37). Otherwise, leave these two options deselected.

**Figure 1.37** WDS Properties—DHCP Tab

21. Go ahead and click **OK** to close the properties tab.

---

You have now successfully set up and configured Windows Deployment Services. We will now take a look at creating a standard server configuration and deploying Windows Server 2008 using WDS.

## Standard Server Image

In this section we will discuss planning and creating standard server images or configurations. These images can be used to ensure all servers follow a standard configuration and can be rapidly deployed on-demand. When considering how many images to set up, you should think about how many “standard” configurations you have in your environment. For example, you may deploy lots of Web servers running IIS and very few SQL Servers. In this case it would make sense to create

a standard Web server image; however, you probably would not want to maintain an image for two or three SQL Servers. You could simply use a base image instead. Keep in mind that you must maintain and update every image you create.

## Automation and Scheduling

Windows Deployment Services (WDS) allow you to use XML files to automate the deployment of operating systems. This process uses an unattend.xml file to automatically select options such as choosing which image to install. WDS will then use the unattend.xml file or a sysprep.inf file to automate the rest of the installation. The unattend.xml is used for Windows Vista or Windows Server 2008. The sysprep.inf file is used for Windows Server 2003 images.

You can use the schedule-cast option to schedule the deployment of images. Schedule-cast is only available as a multicast deployment option. You can configure Schedule-cast to deploy images after a specified number of clients are requesting the image or based upon date and time.

## Certificate Services

Today's organizations must deal with security threats not only from the Internet, but also those from inside their corporate networks. To help ensure data is secured on devices and when transferred between them, many companies have resorted to deploying their own Public Key Infrastructure (PKI). PKIs rely on certificates to provide encryption services and to provide additional security when authenticating people and devices on the network. The most common use of certificates is to provide SSL secured Web sites. You commonly see this when providing payment information online. Certificates can also be used to encrypt e-mail messages, provide two-factor authentication, or encrypt file systems. A good understanding of Certificate Services and how to manage a PKI is becoming an essential skill for network administrators. Microsoft continues to evolve its software products and make them more secure. Many of these products now rely on PKI for ensuring data is transmitted in a secure fashion.

## Introduction to Public Key Infrastructure

Public Key Infrastructure (PKI) was developed and standardized by RSA Labs and other organizations including Microsoft. PKI includes several defined standards known as Public-Key Cryptography Standards (PKCS). These standards use a Public/Private Key process to encrypt and protect data. The following is an example of how Public/Private key encryption works:

1. John and Jane are two people who wish to securely share data.
2. John and Jane each have a key pair which includes a private key and a public key. Private keys are meant to be protected and only accessible to the owner of that private key. Public keys are meant to be shared to make the encryption process possible.
3. In our example let's say that Jane wants to send John a file securely.
4. John first sends Jane his public key.
5. Jane then uses John's public key to encrypt the file.
6. Jane then sends the encrypted file to John.
7. John's private key is then used to decrypt the file. Only John's private key can be used to decrypt the file.

Certificate Services in Windows Server 2008 is Microsoft's solution to deploy PKI in your organization. Certificates are used to associate an identity with a public key. Windows Server 2008 uses certificates that conform to the X.509 standard. X.509 was developed to define a standard set of data that makes up a certificate. This data includes fields such as who issued the certificate, the public key, and dates for when the certificate was issued and when it expires. The following section provides details on how to plan for a Certificate Services deployment using Windows Server 2008.

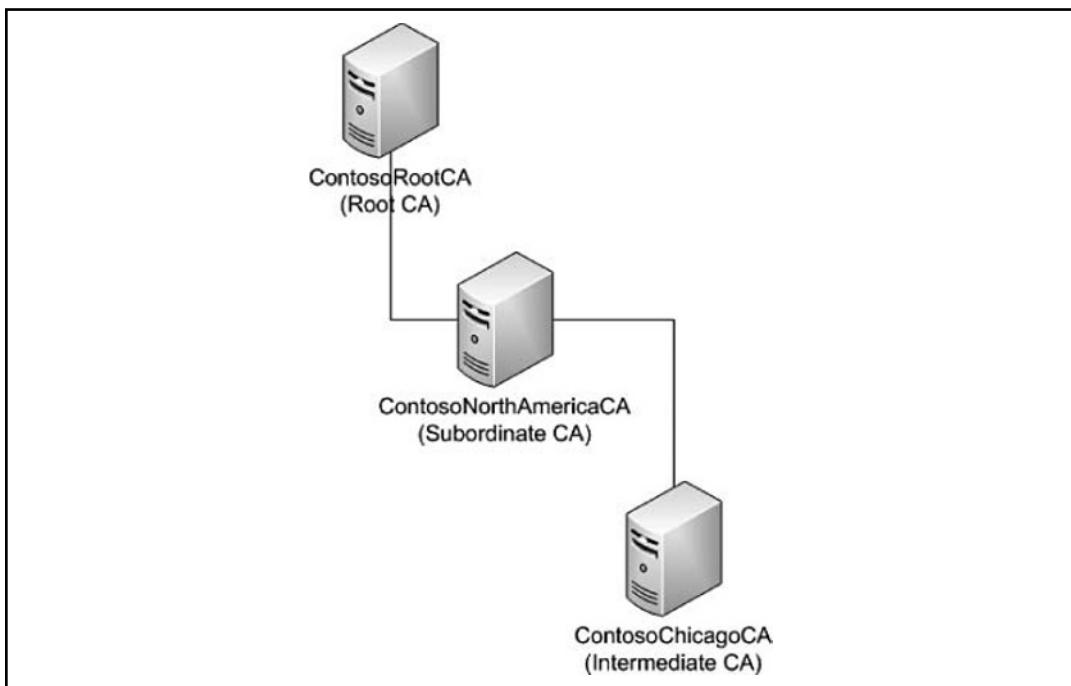
## Planning Certificate Servers

When planning to deploy certificate services, you must make a few key decisions based upon the needs in your organization. One of the critical decisions you must make is whether to deploy a Stand-Alone Certificate Authority (CA), an Enterprise Certificate Authority (CA), or a combination of the two. Certificate Authorities are servers that host the Certificate Services role and issues certificates to users, computers, and other devices. A Stand-Alone CA is easy to setup and configure but provides less features. An Enterprise CA provides a larger feature set, but adds more complexity to management. Enterprise CAs always integrate with and require Active Directory. Enterprise CAs also provide a greater level of security over Stand-Alone as they require Kerberos or NTLM authentication from the requesting user or computer before a certificate will be issued to that entity. You should carefully plan which type of CAs fit best into your organization based upon business needs as well as management costs. If you do decide to deploy Enterprise CAs you should have a good understanding of Active Directory prior to your roll-out. Installation of Certificate Services is performed by using the Add Roles Wizard just like any other server role.

## *Planning Root, Subordinate, and Intermediate Certificate Authorities*

The first Certificate Authority that you deploy in your environment automatically becomes your root CA. The Root CA can then be used to issue certificates to users, computers, or other certificate authorities known as Subordinates. Smaller organizations may choose to deploy only a single CA. This type of deployment is easy to manage and the CA provides certificates directly to users and computers. Some organizations may have the need to deploy more complex CA hierarchies. A hierarchical deployment uses a root CA to deploy certificates to subordinate CAs. The subordinate CAs then provide certificates to users, computers, or other CAs, known as intermediate certificate authorities, below them. Intermediate CAs can then issue certificates to users and computers. Choosing to deploy a hierarchical CA model provides you the ability to maintain more granular control over certificate management as well as segregate CA management for different business units or geographic areas. Figure 1.38 depicts a typical hierarchical CA deployment.

**Figure 1.38** Hierarchical CA Deployment



You need to carefully plan your PKI deployment before setting up CAs on your network. You must also determine which model and type of certificate authorities to deploy. Remember that if you choose to deploy an Enterprise CA, your CA will require Active Directory integration.

## Planning Application Services

Most organizations deploy some kind of centrally managed client-server application services. The most popular of these are Web applications. Web applications have become increasingly popular in today's enterprise. Web applications can be rapidly deployed and can be accessed from any computer or device with a Web browser. Web applications are also usually *WAN Friendly* using small amounts of bandwidth. Microsoft has also introduced a new virtualization platform with the release of Windows Server 2008. Hyper-V is Microsoft's new virtualization hypervisor providing a very scalable and reliable virtualization platform. Each application service deployment requires properly planning before deployment. We will cover both application services in the sections below.

### Planning for Web Applications

Web applications are prevalent on the Internet, corporate intranets, and extranets. Supporting these applications on the Windows platform requires properly planning for the deployment of Internet Information Services (IIS) 7.0. IIS is Microsoft's Web server services added via a server role in Windows Server 2008. IIS 7.0 provides HTTP/HTTPS, FTP, SMTP, and POP3 services. Typically Web applications provide a front-end to data that is stored in a back-end system such as a database.

### Web Farms and Web Site Availability

Web servers can be deployed in Web server farms to provide scalability and availability for Web applications. When deploying Web farms using IIS 7.0 you must decide whether to use Hardware Load Balancing, Network Load Balancing, or Round Robin DNS. Each of these is described below.

- **Hardware Load Balancing** Hardware load balancing offloads the load balancing to a network device instead of the Windows servers. This frees server resources for the Web applications themselves.
- **Windows Network Load Balancing** The Windows Network Load Balancing service provides load balancing services provided by the Windows servers hosting the Web application. Windows Network Load

Balancing adds additional load on the Web servers; however, it is included free with Windows Server 2008. The Windows Network Load Balancing service is easier to set up and configure than most hardware load balancers. Like hardware load balancers, Windows network load balancing provides load-balancing between Web servers and automatic fail-over in the event of a server failure.

- **Round Robin DNS** Round Robin DNS provides load balancing between Web servers but does not provide automatic failover. Round Robin DNS is the easiest to set up and configure as it only requires additional DNS records created.

## IIS Authentication Methods

IIS 7.0 provides a reliable and secure platform for deploying Internet-facing Web applications. Some of your applications may need to be protected by some authentication method to ensure only authorized users access the application. IIS provides several methods of authentication. These include:

- Windows Integrated Authentication
- Kerberos Authentication
- Digest Authentication
- Certificate Based Authentication
- Forms Based Authentication

## IIS Delegation and Remote Administration

Internet Information Services (IIS) 7.0 introduces a new Web server feature known as *Feature Delegation*. This delegation model allows IIS administrators to provide limited administrative functions to developers and Web site owners. Feature delegation allows the developer or Web site owner to configured delegated options via the site's web.config file. For example, as an administrator you may want to allow developers to set the 404 error page to a custom branded one. Feature delegation also allows you to easily update configuration settings for multiple servers in Web farms. Let's say you are deploying a new Web application and need to set authentication type to Kerberos. Traditionally you would have to log on to each server in the farm and set the property within IIS Manager. By using Feature Delegation you can have the developer configure the Kerberos authentication in the web.config file and authentication is automatically set when the Web site is set up on the server.

Remote Administration allows you to take delegation a step further and provide users full access to individual Web sites without giving them physical access to the server or access to other sites. For example, as the network administrator you may want to provide John access to update a Web application on your intranet. In previous versions of Windows you would have to give John full access to all IIS sites to accomplish this. By using Remote Administration in Windows Server 2008, you can now provide John with access to his site only. John can load the IIS manager on his computer and connect remotely to the server. He will then see only sites he has access to.

## IIS 7 Core Server

Like several other roles, Internet Information Services (IIS) 7.0 can be added to a core install of Windows Server 2008. By using a core Web server, you greatly reduce the attack surface of the system. This feature is especially beneficial when deploying Internet-facing Web servers. Like other core servers you will have to manage IIS 7 Core Servers using the command line or GUI tools connected remotely.

## FTP, POP3, and SMTP

IIS 7.0 provides basic FTP, POP3, and SMTP services. File Transfer Protocol (FTP) has been around since the early days of the Internet. FTP was developed to easily transfer files between servers. Many organizations still use FTP today to share files with customers or business partners. FTP provides a great alternative to e-mail when sending and receiving large files.

Simple Mail Transfer Protocol (SMTP) Services are used to deliver e-mail messages within organizations and across the internet. SMTP is the standard communication method for e-mail servers wishing to send and receive messages with other e-mail servers. SMTP is also sometimes used by e-mail clients to send outbound messages to servers. IIS 7 allows you to add a SMTP feature.

Post Office Protocol (POP3) is a standards based protocol developed to allow e-mail clients to download messages from e-mail servers. Using a combination of SMTP and POP3 features, IIS 7 offers a basic e-mail server. Using IIS 7 you can setup and manage e-mail accounts for users within your organization.

## Windows SharePoint Services 3.0

IIS 7.0 can be used to host Windows SharePoint Services (WSS) 3.0. WSS is the core platform for building fully functional collaboration and team sites. WSS provides a central location for users within your organization to share files, participate in online discussions, and manage projects.

## Planning for Virtualization

With the release of Windows Server 2008, Microsoft had made available its new server virtualization service named *Hyper-V*. Hyper-V is Microsoft's first true hypervisor product which provides production grade server virtualization. There are several factors to consider and plan when deploying Hyper-V as a virtualization platform. You must take the following into consideration:

- **Server Resource Usage** How much CPU, memory, and disk does a particular server require physically? Do you have enough resources on the virtualization host to support the system? Though virtualization is a great way to optimize hardware usage, it shouldn't be used as an excuse to skimp on resources needed by a particular application or service.
- **Availability** Due to the fact that you are in a sense placing all your eggs in one basket by running multiple machines on one physical piece of hardware, you should ensure that the physical server is highly available. When deploying Hyper-V host servers you should consider high availability options such as clustering.
- **Management** One of the beauties of virtualization is that it makes servers much easier to manage from a single pane of glass. It makes it so easy in fact that it can sometimes make the environment quickly unmanageable. Hyper-V virtual servers can be deployed very rapidly. You could be tempted to deploy a lot more servers at a much quicker pace than with regular hardware. You should plan for proper procedures and policies for deploying new servers on Hyper-V.
- **Hardware Requirements** Hyper-V requires servers that offer a 64 bit processor and hardware-assisted virtualization. You must ensure your server meets these requirements before deploying Hyper-V on Windows Server 2008.

### EXAM WARNING

Watch out for questions where it may be hard to differentiate between the physical server and virtual server. For example, to add a second hard drive to a physical server requires purchasing an additional drive, correctly ensuring the server can access the new drive, then configuring that drive within Windows. Adding a new drive to a Virtual Server is as simple as using the Add Drive wizard and then configuring the drive within that virtual server.

Microsoft's new Hyper-V virtualization platform allows you to easily set up and manage new servers to consolidate resources and hardware. This not only saves in cost but time spent managing systems. Server virtualization also helps streamline the disaster recovery process of systems. While planning your deployment of Hyper-V you should also consider operating system licensing. Microsoft now allows you to deploy up to 4 virtual instances of the server operating system with the purchase of one Enterprise edition. What this means is you can purchase one copy of Windows Server 2008 Enterprise, and run the physical host and 4 Windows Server 2008 virtual servers on that host without purchasing additional licenses. Let's take a look at installing and configuring Hyper-V on Windows Server 2008.

## Planning for Availability

When planning for Windows Server 2008, you need to take the availability requirements of your business systems. Some systems may require 24/7 uptime, while others may only require availability during business hours. The availability of particular applications or services is typically determined by the business need. You should determine the availability needs of a particular application as it relates to the business organization and deploy availability options based upon those needs. Windows Server 2008 provides several options that provide availability. Let's discuss those in further detail.

## Resilience

Windows Server 2008 provides several options to allow you to deliver resilient and highly available applications and services. Those options include fail-over clustering and network load balancing. Both services should be used in certain situations to provide a highly available system. Typically it is supported to use fail-over clustering on back-end systems such as Exchange mailbox servers, SQL Servers, and even File and Print Servers. Network Load balancing is typically deployed on front-end application servers such as Exchange Transport Servers, IIS Web Servers, and Terminal Server application servers. Fail-over clusters must run on hardware that is certified for Windows Server 2008.

### EXAM WARNING

Be sure you know the key differences between fail-over clustering and network load balancing. Know when to use one over the other. You could see questions that try to mix you up between the two.

## Accessibility

Windows Server 2008 includes several options to enhance accessibility. Features such as magnifier, on-screen keyboard, and narrator make the administration and use of the system more accessible. You can set up and configure all of these options in the new Ease of Access Center located in the Control Panel.

# Planning for File and Print Services

Next to e-mail, File and Print services are one of the most highly utilized services in most organizations today. The availability and performance of servers hosting these services is critical in most companies. During the planning process you must plan for permissions, quotas, replication, searching, and availability. You must also consider which resources you may wish to publish to Active Directory. We will cover each of these more in-depth in the following sections.

## Working with Access Permissions

The concept of access permissions has not drastically changed since Windows NT 4.0. Windows Server 2008 uses the same processes and follows the same rules as previous operating systems. Share and File/Folder permissions allow you to set rights on shares and files. Access permissions ensure only users with proper authorization can open defined files and folders. If you do not properly plan for access permissions, the security management of your files and folders can become a nightmare. In this section we will discuss some of the best practices for managing and working with access permissions.

## Share Level Permissions vs File/Folder Permissions

Windows provides two levels of permissions for access. These are NTFS or File level permissions and Share Level permissions.

- **NTFS Permissions** NTFS permissions are applied at the folder and file level. This means they restrict access to files, whether on the computer or accessing it remotely over the network.
- **Share Permissions** Share level permissions only restrict access to shares that are accessed remotely over the network. This means if you are on the server in which the file is located, Share level permissions will not restrict your access.

Microsoft recommends the use of NTFS permissions when providing user and group access to files. However keep in mind that when using NTFS and Share level permissions, the most restrictive always wins.

## Providing Access to Users and Groups

You can assign access to files and folders to individual users and groups. As a best practice you should use a group to assign access whenever possible. This simplifies the administration model. For example, let's say you have a Tax share that you need to provide access too. Everyone in the accounting department needs access to this share. You could modify the permissions on this share and grant each individual user access. The Microsoft recommended best practice, however, would be to create a global or universal group named Tax Department Users. Then create a domain local group called Tax Share Access. Next you should nest the Tax Department Users group inside of the Tax Share Access group. You would then provide the Tax Share Access group with the appropriate access to the Tax Share. The next time a new tax accountant was hired he would automatically be placed in the Tax Department group and have access to the tax share. There are of course exceptions to the rule. You may find yourself needing to provide only one user access to a folder or share. In this case you may not want to deal with the administrative overhead of dealing with groups. When providing access to a file or share you should be aware of the different levels of access that you can provide to users and groups.

- **Full Control** Full Control means just that. Users with full control can do just about anything to the folder. Users can read, write, make changes, take ownership, and even delete the folder itself. Be careful with Full Control and only provide non-administrators this level of access when absolutely necessary.
- **Write** Write permissions allow the user to save new files to a folder by copying them there. Unless the users are also granted read access they cannot see and open documents within the folder.
- **Read** Read permissions allow users to see and open files within a folder. They cannot make changes to files and folders with this level of access.
- **List Folder Contents** List Folder Contents permission allows users to see the names of files within folders; however, they cannot open those files.
- **Read and Execute** Read and Execute provide the same level of access as read permissions with the addition of the ability to traverse folder structures even if they do not have the rights to parts of the folder path.

- **Modify** Modify permissions allow users to read, write, and delete. Like the full control permission, this level of access should be used cautiously and only allowed on folders where the users need the ability to delete folders.

When planning your Windows Server 2008 deployment you should document all folders and proper permissions. You should use groups to provide access to the folders and shares on your network.

## Allow and Deny

Both Share and NTFS permissions provide the ability to allow and deny access to a share, folder, or file. If *allow* is not enabled then access is always implicitly denied. However, if *deny access* is explicitly set then it always wins. A *deny* and *allow* always equals *deny*. For example, if you provide the operations group with *write* access to a share on the network and then choose to explicitly set the *deny* permission for write access, then *write* will win. Microsoft does not recommend using the *deny* permission except in special situations. For example, the marketing group has *modify* permissions on the Marketing share. Joe in HR needs *read* access to the share temporarily. You could place Joe in the marketing access group and then set the share to *deny* access to Joe for all permissions except read. Keep in mind though, that typically the use of *deny* on a regular basis points to poor access planning. Let's go ahead and walk through configuring permissions. In our example we have a user named John Smith who is a member of the Boston Accountants global group. The Boston Accountants global group is a member of the Tax Files Access group. We will be creating a new share in which we will provide John access. We will follow best practices by assigning permissions to the Tax File Access group. Permissions will be setup in this manner: John Smith ® Boston Accountants ® Tax File Access ® Tax Share. Let's go ahead and proceed with the exercise.

### EXAM WARNING

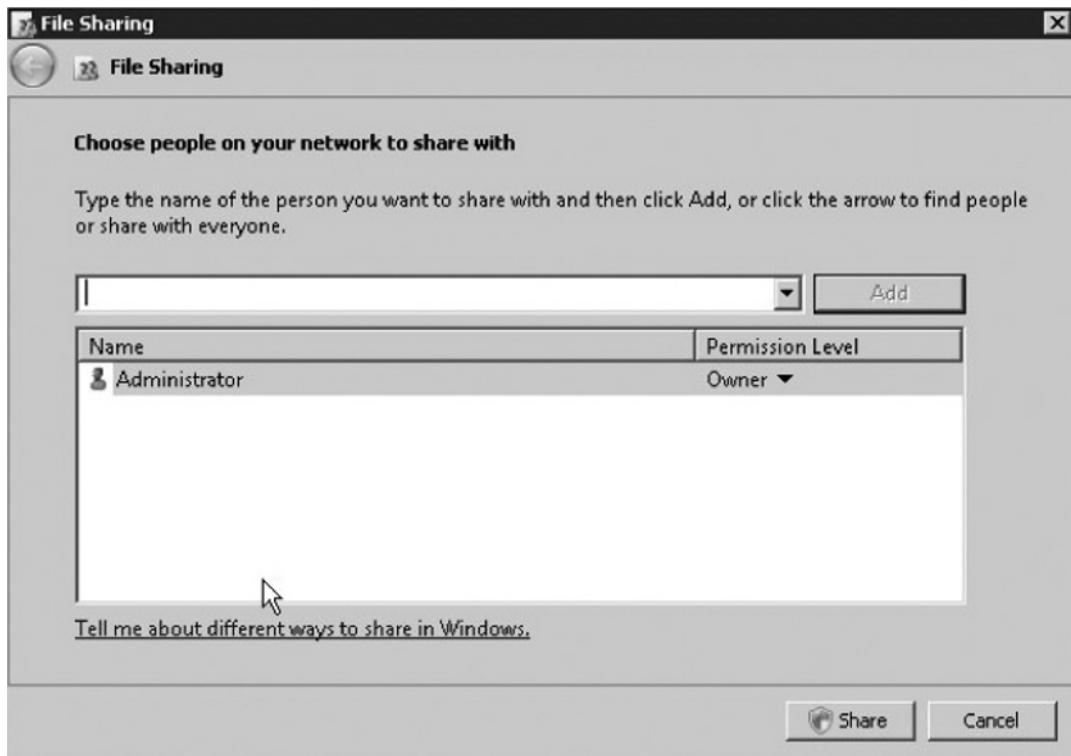
Be ready for several questions related to access permissions. Make sure you have a very good understanding of Allow and Deny. There could be a trick question or two around the use of the *deny* permission.

## EXERCISE 1.5

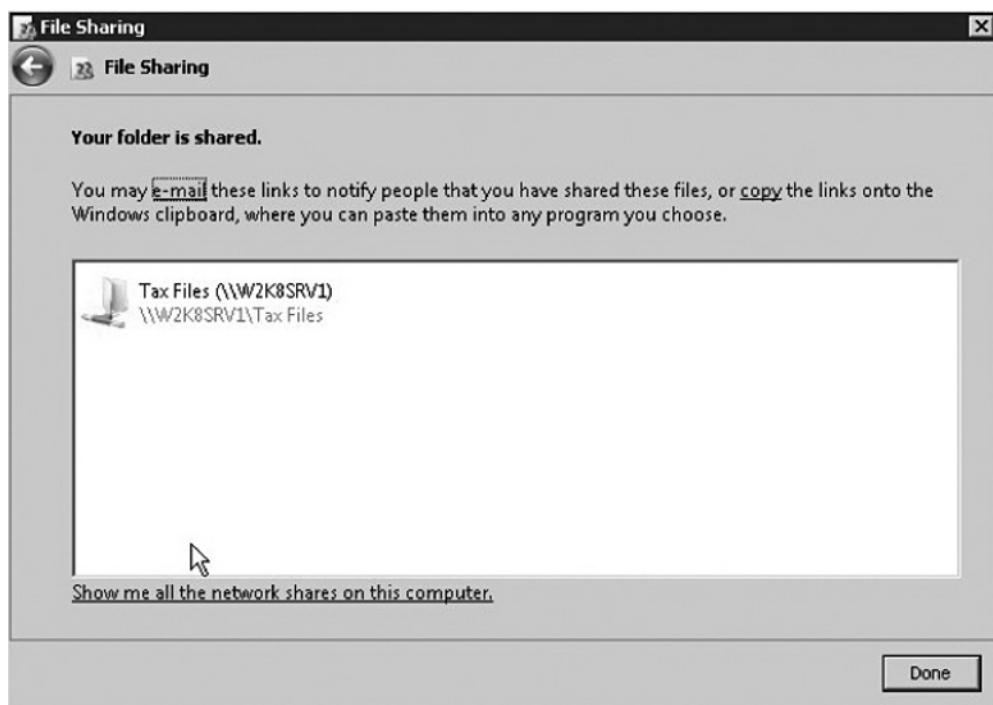
### CONFIGURING NTFS PERMISSIONS

1. Create a new folder named **Tax Files**.
2. Right-click the folder and select **Share**. This will launch the **File Share** dialog as seen in Figure 1.39.

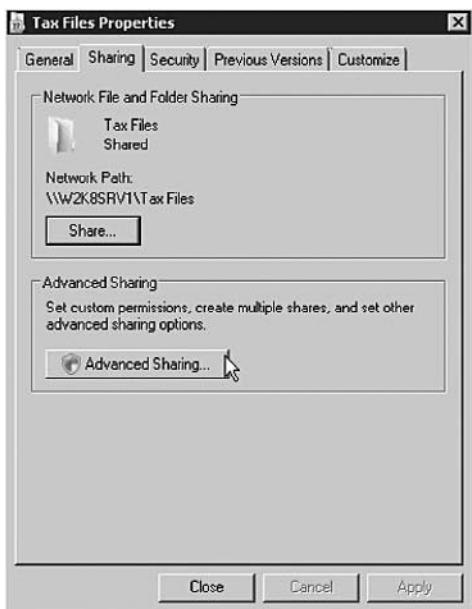
**Figure 1.39** Create File Share



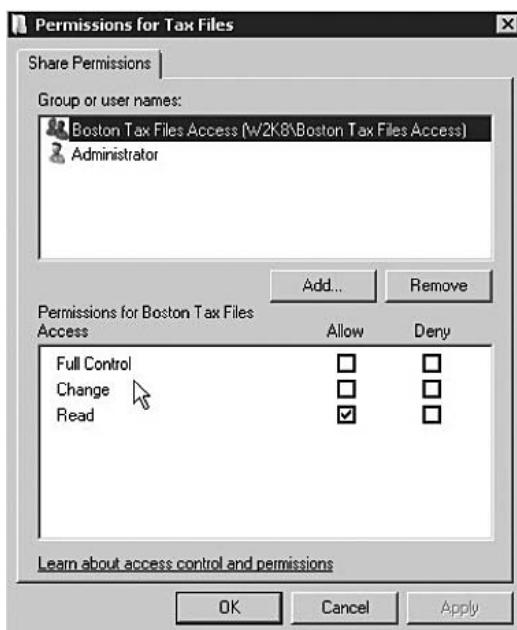
3. Add the **Boston Tax File Access** group. Then click the **Share** button. The share will be created and you will see a confirmation as seen in Figure 1.40. Click the **Done** button to close the dialog window.

**Figure 1.40** File Share Created

4. By default, the process above just granted read and execute access to the Boston Tax File Access group. However, we want to provide write access to this group. Right-click the newly shared folder and select **Properties**.
5. In the **Properties** dialog box click the **Sharing** tab. Then click the **Advanced Sharing** button as seen in Figure 1.41.

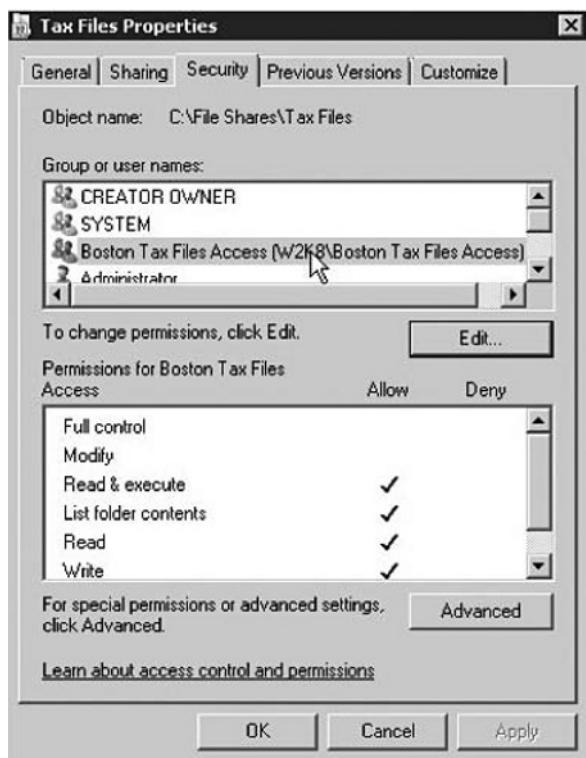
**Figure 1.41** Modifying Share Level Permissions

6. In the **Advanced Sharing** dialog, click the **Permissions** button. Notice the Boston Tax Files Access group only has read permissions (See Figure 1.42).

**Figure 1.42** Boston Tax File Access Share Permissions

7. Go ahead and select **Full Control** for the Boston Tax Files Access group. Then click the **OK** button. Click **OK** again to return to the **Properties** window. Remember the permissions for a folder are the most restrictive of share level and file level permissions. We will restrict access to modify at the file level which makes it okay for us to go ahead and provide full control at the share level.
8. Click the **Security** tab. From here you can see the **Boston Tax Files Access** group has only Read and Execute permissions (See Figure 1.43).

**Figure 1.43** Boston Tax File Access NTFS Permissions



9. Click the **Edit** button to allow us to grant the group modify permissions. Go ahead and select the **Boston Tax Files Access** group. Then select the **Modify** option. Then click the **OK** and **Close** buttons. You have now provided John Smith with the appropriate modify permissions on the Tax Files share. Browse to the share and make sure John Smith can now access and make changes to the share.

## Storage Quotas

Storage Quotas allow administrators to limit the amount of storage used by end users. This helps ensure users are properly using business-related storage. Storage quotas work a lot like e-mail quotas. Users are given a limit on the amount of data that they can store in a specific location. If they reach this limit they can be sent a warning message or prevented from saving new files to this location.

These quotas can be set on a volume or folder level. For example you may use home drives or redirect the My Documents folder to a network share in your organization. You can set up each user to only be able to save 2 GB of data to her home drive or My Documents folder. You could then set up Windows to e-mail people when they have used 90% of their quota so they know to delete or archive some of their old files.

If your organization needs to control the use of storage resources then you should properly plan and deploy storage quotas. Storage quotas should be set up in line with company storage policies.

## Planning for Replication

Windows Server 2008 allows you to replicate shares and their contents between servers. This feature is known as Distributed File System Replication (DFSR).

DFSR allows you to replicate a share and its contents between servers. This feature is especially useful in two situations:

1. **Disaster Recovery (DR) and Backups** If you have branch office locations with file servers, you can use DFSR to replicate all files from those servers to a central hub server. You can then back up those files from the central hub server instead of placing a backup system and process in each branch office. DFSR replication is also useful to ensure data is being replicated offsite. If the branch office server crashes you can simply direct the users to the same share on the hub server in the main office location.
2. **File Distribution** You can use DFSR to easily replicate files from a central storage location to remote branch office files servers. For example, you may have a share in each office that is used to host software installation files. Instead of ensuring those files are maintained and updated in each location, you could simply set up a hub server and update and add new software installations to that server. The hub would then replicate those files to each branch office file server.

Replication provides lots of possibilities to assist organizations with file server management and disaster recovery.

## Indexing Files

Windows Server 2008, like Windows Vista, includes the new Windows Search Service. Previous versions of Windows included the ability to search for files and folders. However, these searches were always performed directly against the file system instead of an index. The search process was slow and at times could cause extensive disk I/O.

Windows Search in Vista and Server 2008 introduced search using an index file which is updated and maintained in real-time. This process is similar to the way database systems index their tables. The index process in Vista and Server 2008 throttles itself so that it does not contend with other applications and services on the server. When you perform a search against this index minimal resources are used and results are quickly returned. By default the Windows Search Service indexes Microsoft Office Files, Images, Videos, Text Files, as well as Microsoft Outlook content. The Windows Search Service is extensible. Developers can write extensions known as IFilters to allow the service to index other file types. The Windows Search service can also be used to search against remote indexes on Internet Search engines and other Microsoft applications such as Office SharePoint Server 2007.

When planning your Windows Server 2008 deployment you should take the Windows Search Service into consideration. By deploying both Windows Vista and Windows Server 2008 you can achieve quick and reliable searches of file servers. You can configure Windows Server 2008 to index the file shares it hosts. You would then configure Vista clients to point to these indexes which in return would allow the client to quickly search for files and folders on the server's shares. If you do decide to use indexing of your file shares as a search mechanism you must ensure the core services for Search remain healthy and available.

## Storage Policies

Windows Server 2008 allows you to implement storage policies, otherwise known as file screens, to block certain file types from being saved in locations in which the policy applies. For example you could create a file screen that prevents users

from saving audio and video files to a network share where accounting information is stored. File screening can be implemented in an active or passive mode. Active screening will actually prevent users from saving the screened file type to the location, while passive screening will only perform an action or alert when a user saves a screened file type to the specified location. File screening can be very useful to ensure users are saving certain files types in correct locations or to prevent users from saving files on the network that shouldn't be there.

## Understanding Availability Options

Windows Server 2008 file servers can take full advantage of the availability features provided by fail-over clustering and DFSR. Each of these features should be evaluated as options to provide high availability for your file servers.

### File and Print Server Clustering

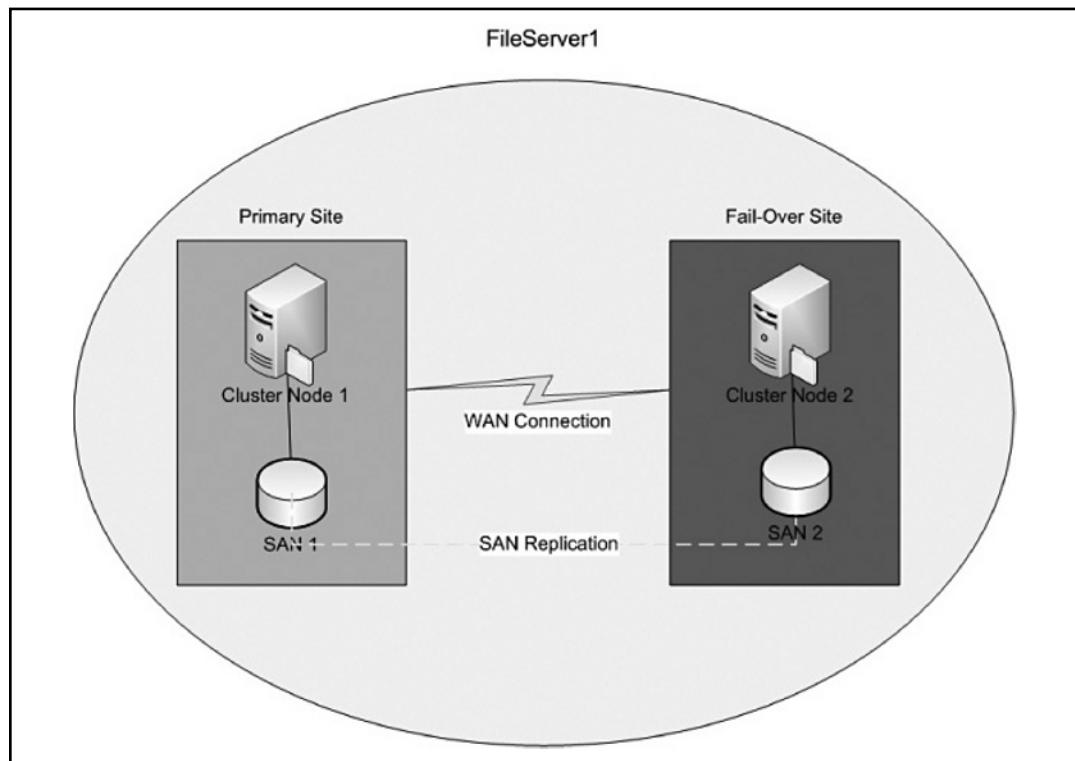
File and Print Server clustering in Windows Server 2008 allows you to provide highly redundant file and print servers with automatic fail-over. If the primary server goes offline, the secondary server almost instantly becomes available. End users experience little or no loss of connectivity. File and Print server clustering has been available in previous version of Windows Server and has proven itself as a great way to minimize downtime. The one problem with previous versions of Windows clustering has been that it was somewhat complicated to set up and manage. Windows Server 2008 addresses this problem by providing configuration wizards and validation checks. The following are some key requirements for setting up File and Print Server clusters in Windows Server 2008.

- **Shared Storage** Clusters must use shared storage. Typically this is a Fibre Channel or iSCSI SAN.
- **Windows Server 2008 Enterprise or Data Center Edition**
- **Like Hardware** Servers that are members of the cluster must have like hardware. Only Certified Windows Logo hardware can be used to create Microsoft supported clusters.

Windows Server 2008 can provide highly available File and Print Servers over Wide Area Networks (WAN). By creating GeoClusters, file and print servers can

remain online even if the entire primary site goes offline. Figure 1.44 depicts a typical GeoCluster using Windows Server 2008.

**Figure 1.44 A Typical GeoCluster Using Windows Server 2008**



Let's discuss the above diagram a little more in detail. Let's assume we have two sites. Our primary site is located in New York and our secondary or Fail-Over site is located in Chicago. Our Chicago users access the file server named FileServer1 extensively. In the diagram above we will be using two cluster nodes or servers. Each cluster node uses a Storage Area Network (SAN) for disk storage. User files are stored on a disk drive which is located on the SAN. We then use SAN replication technology to replicate those files to SAN 2 in the

Chicago Fail-over site. Cluster Node 2 is connected to SAN 2. Now let's assume that the server Cluster Node 1 has a bad memory stick and goes offline. Cluster Node 2 immediately takes over control and continues to present file shares under the name FileServer1. End users will experience little or no loss of connectivity. The above diagram provides a brief overview of how Windows Server 2008 GeoClusters can work to provide highly available File and Print Servers. The entire primary site could be offline and users could continue to access shares on FileServer1.

## Publishing Printers

Windows Server 2008 allows you to publish printers to Active Directory. This allows users to easily search for and locate printers on the network. Printers can be published with information such as name, location, and capabilities. For example, you can publish a new color laser printer to Active Directory. If a user searches for a printer with color capabilities, the newly published printer will show up in the results.

## Summary of Exam Objectives

Planning is one of the most critical and most often overlooked steps to any server deployment. This is no exception in Windows Server 2008. You must properly plan for deploying the operating system and decide whether to upgrade existing servers or perform a clean install on new servers. If you are building a new network, you must plan for all related infrastructure services. DNS, DHCP, NAP, and Active Directory are all critical components to your organization's IT infrastructure. Proper planning is crucial before deploying these services or you could end up having to rebuild your network. New technologies such as BitLocker, Read-only Domain Controllers, and the Windows Firewall allow you to ensure your server deployment is secure and reliable. You should also properly plan for high availability scenarios when necessary. You must know when to deploy network load balancing over fail-over clusters and what features each provides. You should also now have a good understanding of how to set up and properly manage a file server and permissions. This chapter covered a lot of key elements required to properly maintain a Windows server infrastructure. Make sure you have a good understanding of all topics we discussed in this chapter.

## Exam Objectives Fast Track

### Planning for Installation and Upgrade

- You must determine which Windows Server 2008 edition should be deployed to fulfill a particular business requirement.
- You should determine if you want to upgrade existing servers or perform a clean installation.
- Server hardware must meet Windows Server 2008 hardware requirements before the operating system can be installed.

### Planning for Automated Server Deployment

- Windows Deployment Services provides features to rapidly deploy Windows Server 2008.
- Windows Deployment Services requires DNS, DHCP, and Active Directory.
- You can use Windows Deployment Services to install an operating system through normal setup or deploy a prebuilt image.

## Planning for Infrastructure Services

- Windows Server 2008 offers key infrastructure services such as DNS, DHCP, NAP, and Directory Services.
- DNS and DHCP are easy to setup and configure but must be properly maintained to ensure a healthy network.
- Active Directory requires extensive planning to determine the best model for your organization.

## Planning Application Services

- Windows Server 2008 provides new application services such as IIS 7 and Windows Server Virtualization.
- High availability options such as Network Load Balancing and Fail-over clustering can be used to provide reliable and scalable applications.
- Windows Server Virtualization can be used to run multiple instances of the Windows Operating System on a single server.

## Planning for File and Print Services

- Users and groups should be used to assign permissions to shares on file servers.
- Storage Policies and Quotas can be used to control how much data and what types of files users can save to network shares.
- Network printers can be published to Active Directory so that they can be easily located.

# Exam Objectives

## Frequently Asked Questions

**Q:** Can you upgrade existing Windows Server 2003 computers to Windows Server 2008?

**A:** Yes, you can choose to upgrade the existing Server 2003 operating system or perform a clean install of Windows Server 2008.

**Q:** Can you use WDS to perform unattended installs of Windows Server 2008?

**A:** Yes, you can configure WDS to use unattended install files to automate the installation of the operating system.

**Q:** How do you determine how many Active Directory domains and forests are needed in a typical deployment?

**A:** Most organizations can operate with a single forest and domain; however, the determining factor is typically security boundaries. Some companies may require separate enterprise administrators for different business units or geographic locations. These all must be considered when planning an Active Directory deployment.

**Q:** How do you determine when to use Network Load Balancing over Fail-Over clustering?

**A:** Network Load Balancing is typically used for front-end servers such as Web servers or terminal servers, while Fail-over clustering is used on back-end systems such as SQL Server or Exchange mailbox servers.

**Q:** When deploying Windows Server 2008 file servers, what is the best way to assign permissions to shares?

**A:** You should use groups to properly manage users and assign permissions to shares. You should also use NTFS permissions over share level permissions when possible. Use the deny permission very sparingly.

## Self Test

1. Your wireless network uses WEP to authorize users, but you also use MAC filtering to ensure that only preauthorized clients can associate with your APs. On Monday morning, you reviewed the AP association table logs for the previous weekend and noticed that the MAC address assigned to the network adapter in your portable computer had associated with your APs several times over the weekend. Your portable computer spent the weekend on your dining room table and was not connected to your corporate wireless network during this period of time. What type of wireless network attack are you most likely being subjected to?
  - A. Spoofing
  - B. Jamming
  - C. Sniffing
  - D. Man in the middle
2. You are planning to upgrade to Windows Server 2008 and want to reuse existing servers only if they meet the recommended hardware requirements. During an assessment of your current servers you determine they all have a standard configuration of 80 GB hard drive, dual 3.0 GHZ processors, and 1 GB of memory. Can you proceed to use the existing hardware? If not, what component must be upgraded?
  - A. No, the hard drive must be upgraded to at least 100 GB
  - B. No, the memory must be upgraded to at least 2 GB
  - C. No, the CPU must be upgraded to at least 3.2 GHZ
  - D. Yes, the current hardware configuration can be used
3. While planning your Windows Server 2008 deployment you determine you need to deploy two servers in your main office to support a SQL cluster. Which editions offer this capability? (Select all that apply)
  - A. Standard Edition
  - B. Enterprise Edition
  - C. Web Edition
  - D. Data Center Edition
  - E. Itanium Edition

4. Your security team has mandated that all new deployments of server operating systems must use BitLocker to provide disk level encryption. Which editions of Windows Server 2008 support disk encryption? (Select all that apply)
  - A. Standard Edition
  - B. Enterprise Edition
  - C. Web Edition
  - D. Data Center Edition
  - E. Itanium Edition
5. Before upgrading to Windows Server 2008 you are required to provide a roll-back plan to management. You must describe the process and tools used to perform the rollback in case of upgrade failure. What built-in tool can you use to rollback changes made by an upgrade to Windows Server 2008.
  - A. System Restore
  - B. Backup Wizard
  - C. Remote Assistance
  - D. Performance Monitor
6. You have decided to use Windows Deployment Services (WDS) to manage your operating system deployments. Before setting up WDS you want to ensure all infrastructure requirements are already met. What infrastructure services must you ensure are available before setting up WDS? (Select all that apply)
  - A. DNS
  - B. DHCP
  - C. RADIUS
  - D. Active Directory
  - E. IIS
7. You recently set up DHCP to supply IP addresses to all workstations on your network. All workstations at corporate headquarters, where the DHCP server is located, are receiving IP addresses properly. You have confirmed that servers

with static IP addresses in the New Jersey office can connect to headquarters. However no workstations in the branch office in New Jersey are able to obtain IP addresses. What is the most likely cause of this problem?

- A. The WAN is currently down and the DHCP server is unreachable by the clients.
  - B. The DHCP Server is offline.
  - C. A DHCP Server must be set up in the Branch Office.
  - D. The DHCP Server is not configured properly.
8. You want to deploy Network Access Protection (NAP) to ensure all client computers have current software updates installed before connecting to the network. Your clients consist of Windows 2000 Service Pack 4, Windows XP Service Pack 2, Windows XP Service Pack 3, and Windows Vista. Which clients must you upgrade before deploying NAP? (Select All That Apply)
- A. Windows 2000 Service Pack 4
  - B. Windows XP Service Pack 2
  - C. Windows XP Service Pack 3
  - D. Windows Vista
  - E. None of the clients need to be upgraded
9. You are deploying Active Directory to provide directory services to your organization. Your Active Directory deployment will support 100 users and around 90 client workstations. The 90 users consist of three departments (accounting, human resources, and IT). All users and computers are located in one office and supported by a centralized IT Department of two Network Administrators. What is the best way to deploy Active Directory for this organization?
- A. Deploy a single forest and domain for the organization.
  - B. Deploy a single forest with a parent domain and a child domain for each department.
  - C. Deploy a separate forest and domain for each department.
  - D. Deploy a separate forest for each department and use a single domain.

10. You are designing your domain controller deployment strategy and determine all branch offices need a domain controller at that location due to slow and sometimes unreliable WAN links. Your security team is somewhat concerned about placing a domain controller in the Toronto office as there isn't a very secure location to physically store the server. What feature in Windows Server 2008 will allow you to place a domain controller in the Toronto office and ensure that no administrator accounts are stored on that server?
- A. Global Catalog
  - B. Storage Policies
  - C. BitLocker
  - D. Read-Only Domain Controller

## Self Test Quick Answer Key

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

This page intentionally left blank

# Chapter 2

## MCITP Exam 646

### Planning for Server Management

#### Exam objectives in this chapter:

- Developing a Management Strategy
- Delegating Administration
- Planning a Group Policy Strategy
- Creating and Linking Group Policy Objects
- Controlling Application of Group Policies

#### 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 common challenge that presents itself to administrators from many IT organizations is the ability to effectively and adequately manage the servers in their enterprise. In order to be successful at server management your first priority should be to take the time to map out a sever management plan. A server management plan typically will include information that answers the following types of questions:

- What tools will you use to administrate your servers?
- Who will be allowed to administrate?
- In what fashion will the administrators connect?
- Will server lockdown via policies be enforced?
- How will delegation be addressed?

A server management plan ensures that you choose the appropriate management tools and management configurations for your organization. To develop your plan, you first need to know the server configuration in your organization: where the servers are located, what roles they perform, and what operating systems they are running. You also need to know the availability requirements for the servers you plan to manage remotely and who the application owners and administrators are. You must take the time to address all the impacts on your infrastructure in order to be able to provide proper management. Once you have collected the appropriate information from your environment you will be able to plan the regular management tasks to be performed, and when and how often they should occur.

In this chapter you will learn about some of the different types of server management tools and methods available to you in Windows 2008. Topics will include remote administration, group policy, and delegation strategies which can all be used to assist you in the day to day of server management.

# Developing a Management Strategy

In order to ensure that your servers run optimally you must develop a management plan that outlines the management tasks required in your organization and the tools that will be used. The frequency of the identified tasks will vary across different enterprises as well as within the same enterprise but across different server types. There will be some tasks that will need to be run on a frequent scheduled basis, like Backups, and others which will need to be run less frequently but still scheduled

such as Disk Defragmentation. Some tasks even fall into the “run once” category for a particular server. Regardless of what the tasks and tools encompass the first step is always to examine the existing environment and identify the need for management. Once pain points have been fleshed out tools can be thrust into active to perform the critical actions which keep your servers humming like well-oiled machines. Since planning a management strategy is the goal here we will discuss some of the available tools in Windows Server 2008 that may help you to command and conquer in your enterprise.

## Remote Administration

Administrators typically do not stage their workspaces in the company’s server room. One reason would be that most server rooms are cold which makes them somewhat uncomfortable to work in for long periods of time. Another reason would be that it can be hard to hear other human beings while standing in a server room full of blaring fans and A/C units. Typically though the most imperative reason that administrators don’t make their homes in server rooms would be that real estate with raised floors and redundant power is valuable and having an administrator plop pictures of his kids here and there and make themselves at home just doesn’t add up.

So what does an administrator do? You have a desk or cubicle just like anyone else in the company. So what happens when you need to log on to a server in the environment? You could walk to the server room (or drive in some cases), and then once you have arrived take the time to locate the machine you want to work on. The probability is that you won’t know where it is racked so it may take some digging around to locate it. Once you locate it now you have to wrangle with the KVS to get the proper server up on the monitor, mouse, and keyboard, and even then there is a reasonable chance that things may not work as expected. So once you finally get to the datacenter, find the right server, get logged onto the KVS, and get the right server selected in the KVS system you are finally to the point that logon can begin. You haven’t really done any work so far, yet you feel like you have run a short marathon and are ready for a coffee break.

Obviously this isn’t the best way to go about things—so what is? Remote administration. Many administrators perform their day-to-day functions sitting at their desk utilizing some form of remote connectivity to their servers. By planning for remote administration methods in your environment you create the flexibility required to sit anywhere on your network and still have the ability to perform your

job function by connecting to the servers. The two primary methods of remote administration in Windows Server 2008 are:

- Remote Desktop Protocol (RDP)
- Remote Server Administration Tools (RSAT)

RDP has been around for some time in Microsoft technologies and has had a bit of a makeover with Windows 2008 which we will discuss. The RSAT collection of tools is what used to be referred to as the ADMINPAK.MSI. RSAT is the new name for a familiar face and many of the tools still exist within RSAT as they were in ADMINPAK.MSI, but they have been joined with a list of new and interesting utilities pertinent to Windows Server 2008. Here is a list of what is included with RSAT:

- Role Administration Tools
  1. Active Directory Certificate Services (AD CS) Tools
  2. Active Directory Domain Services (AD DS) Tools
  3. Active Directory Lightweight Directory Services (AD LDS) Tools
  4. DHCP Server Service Tools
  5. DNS Server Service Tools
  6. Shared Folder Tools
  7. Network Policy and Access Service Tools
  8. Terminal Services Tools
  9. Universal Description, Discovery and Integration (UDDI) Services Tools
- Feature Administration Tools
  1. BitLocker Drive Encryption Tools
  2. Failover Clustering Tools
  3. Group Policy Management Tools

4. Network Load Balancing Tools
5. SMTP Server Tools
6. Storage Manager for SAN's Tools
7. Windows System Resource Manager Tools

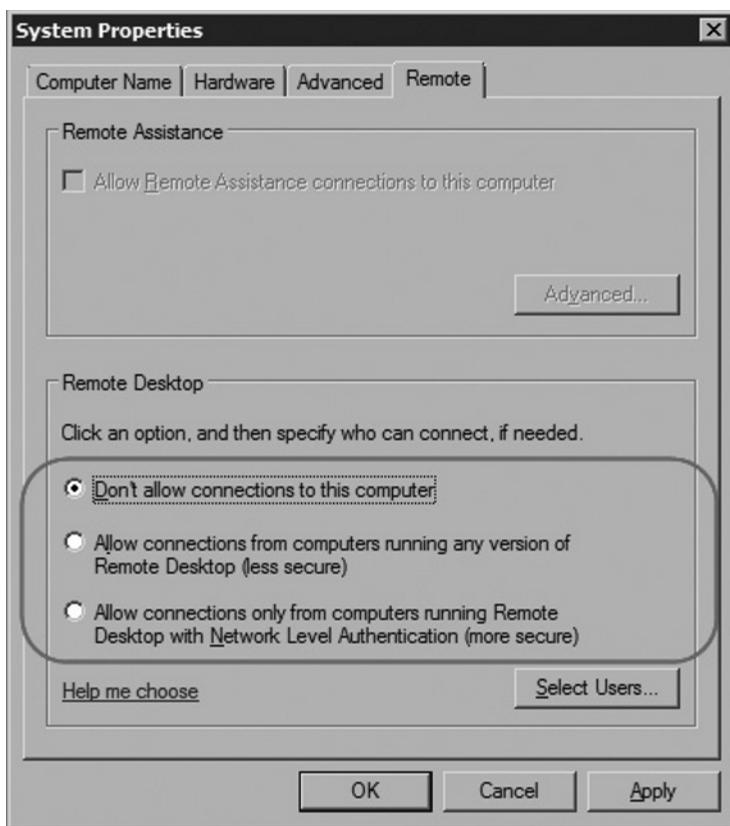
The RSAT tool set will be a useful addition to many administrators' toolkits, but I do want to point out that connecting to a server via Remote Desktop would yield all the tools relevant to the Roles and Features installed on that particular server. That being said we are on to discuss the ever so useful Remote Desktop!

## Remote Desktop

Remote Desktop allows you to connect to any machine in the network as if you were sitting in front of its monitor, mouse and keyboard. The Remote Desktop Protocol (RDP) is the protocol that makes remote desktop connectivity possible and allows you to perform most of your day-to-day administration without ever leaving your desk. It is a lightweight protocol that transfers user input and server output between the client and server. No data actually transverses the wire via RDP—for instance, mouse clicks or keyboard strokes in an Excel spreadsheet may be sent to the server, but not the XLS file in which those actions occur. The benefit in this is that RDP is viewed as a safe and secure protocol in which to remotely administer your servers. Since no data content crosses the wire between client and server it protects the server from exposure and potential vulnerability.

By default in Windows 2008 Remote Desktop is not enabled and it must be configured to allow usage. You must be a member of the local Administrators group in order to enable Remote Desktop. In order to enable Remote Desktop perform the following steps:

1. Click **Start** | Right-click **Computer** | Click **Properties**.
2. Select the **Remote** tab.
3. On the **Remote** tab you have three options for **Remote Desktop** as shown in Figure 2.1.

**Figure 2.1** Configuring Remote Desktop Options

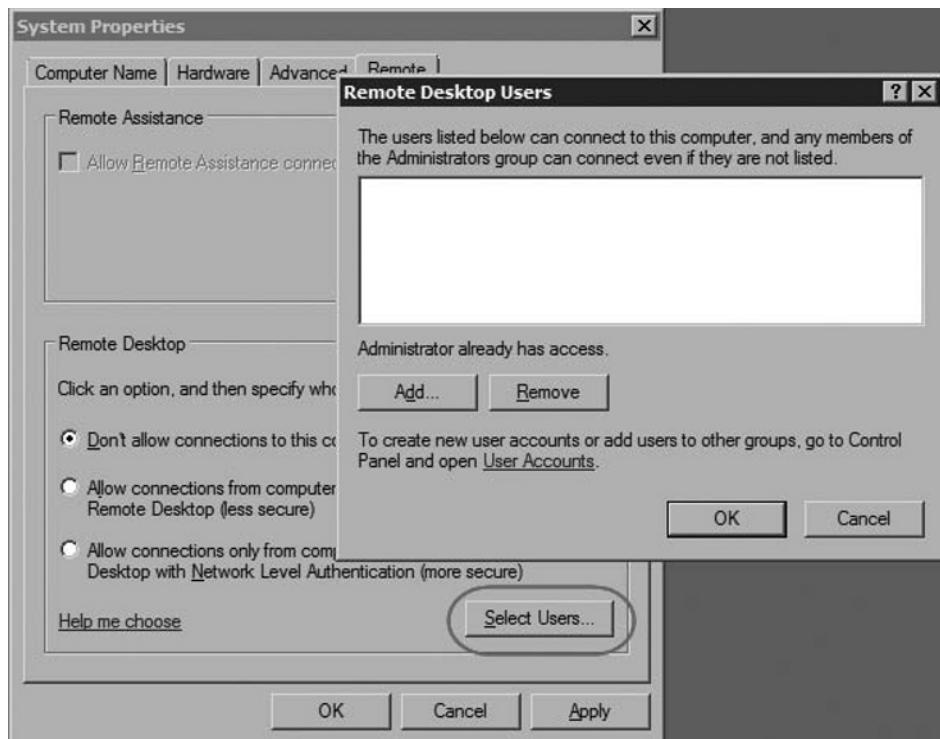
There are two options available to enable Remote Desktop and which one you select depends on the clients existing in your enterprise. The middle radio button, **Allow connections from computers running any version of Remote Desktop (less secure)**, will most likely be your choice. Any version of the Microsoft Terminal Services client is allowed to authenticate when this option is selected. Since most networks are still a mixture of client operating systems this option would make the most sense initially. Once your network has for the most part migrated to Windows Vista then it would be time to flip the switch to the third radio button, **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**. This option only allows machines to connect that can take advantage of the Network Level Authentication feature built into Windows Vista. Essentially you are authenticated *before* being taken to the logon screen.

## EXAM WARNING

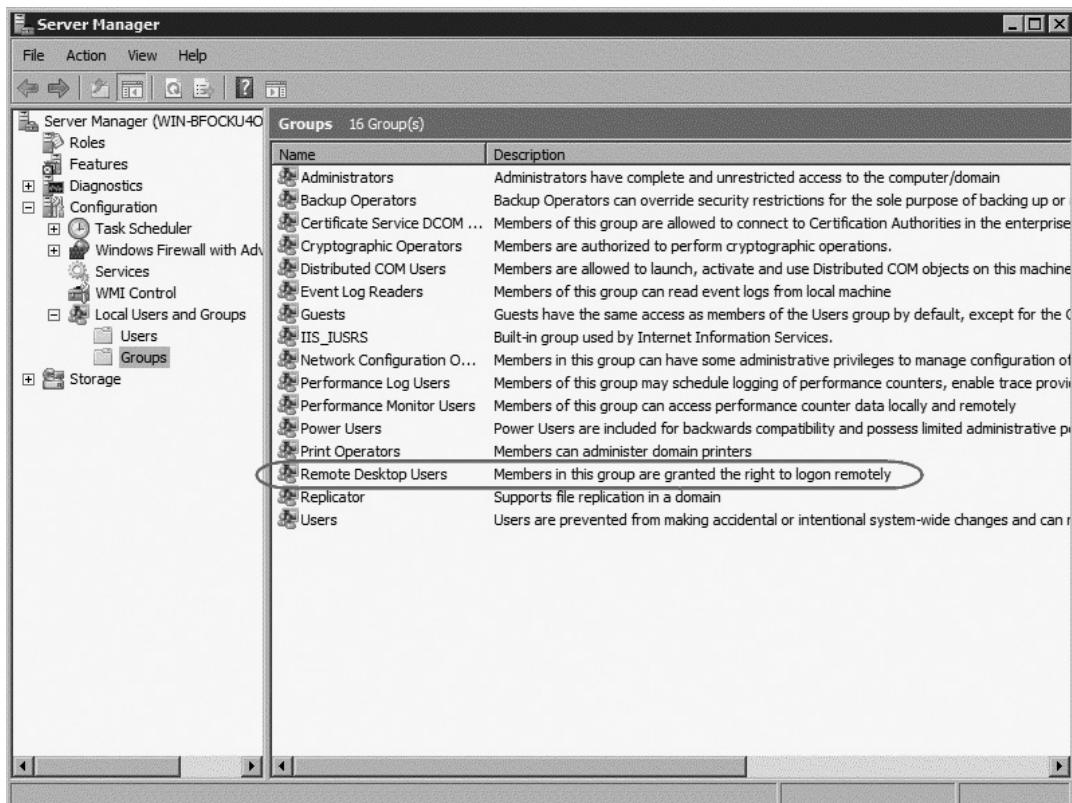
Only three simultaneous connections are allowed into a machine with Remote Desktop enabled: two sessions plus the console session. These connections are intended for administrative purposes. For the ability to connect and launch non-administrative applications or to connection with more than three simultaneously connections you should install Microsoft Terminal Services.

So once you have enabled Remote Desktop you must now decide which accounts are to be granted permission to log on. By default all members of the local **Administrators** and the **Remote Desktop Users** (see Figure 2.2) groups are granted rights to log on via Remote Desktop automatically, but any additional users must be explicitly granted permission (see Figure 2.3).

**Figure 2.2** Granting Additional Users Remote Desktop Permission



**Figure 2.3 Remote Desktop Users Group**



So now that you have successfully enabled Remote Desktop the next thing to do is to connect via the Remote Desktop Connection client and administrate! In order to connect to a server you must have a client available to you. Microsoft has included the Microsoft Terminal Services Client (MSTSC) in their operating systems so that there isn't anything additional to install on your workstation in order to start connecting. However, native to Windows Vista with SP1, Windows Server 2008, and Windows XP with SP3 is the MSTSC 6.1 client, also known as Remote Desktop Connection (RDC) 6.1. This version of the terminal services client offers some new features:

- Server authentication
- Resource redirection
- TS Gateway servers
- Monitor spanning

- Terminal Services Remote Programs
- Visual improvements

The features available will depend on what has been configured, for instance, TS Gateway servers must be installed for a TS client to take advantage of the service. Other new features, like Resource redirection and Visual improvements will always apply and do not require additional configuration to be active.

All in all Remote Desktop is a critical tool in any environment. The ability for an administrator to transport themselves onto a server without ever leaving their desk is worth its weight in gold, but the additional capabilities of the new incarnation of Remote Desktop and the Remote Desktop Client put the real shine on this newly improved piece of Windows Server 2008. By adding security (via Server Authentication and Network Level Authentication), flexibility (via Monitor Spanning and Resource redirection), and finally portability (via TS Gateway services and Terminal Services Remote Programs) to the already incredibly useful Remote Desktop component Microsoft has made a good showing. Besides bringing a lot of new functionality to the table for administrators they have also appealed to your best interests—the interest in being able to work from home with additional ease!

## Server Management Technologies

Much to the delight of the IT world, Windows Server 2008 has been developed chock full of many new management technologies and features. Some of these include new Server Management Technologies include:

- Revised **Server Manager** tool
- **Windows PowerShell**
- **Windows Deployment Services**
- **Windows Reliability and Performance Monitor**

Server Manager will be discussed in the next section, and we will describe the others here.

## Windows Powershell

Windows Powershell is a command line world which allows you as the administration a multitude of power and control over your Windows environment through scripting. Windows PowerShell introduces the concept of a **cmdlet**. A **cmdlet** is a single-function command-line tool built into the shell used to perform administrative actions of all kinds. Even with very limited scripting knowledge any administrator

can soon be right at home in a Powershell interface. With standard command line tools built in and an extension help infrastructure Microsoft has made it easy for any administrator to assume control over automation in their environment.

## Windows Deployment Services (WDS)

Windows Deployment Services is the new and improved version of the Remote Installation Services (RIS) that existed in previous Windows incarnations. WDS's purpose in life is to allow you to deploy Windows operating systems. WDS includes support for Windows Vista and Windows Server 2008. You can take advantage of WDS services to provide OS deployment services—for both Windows Vista and Windows Server 2008—in your environment. It utilizes Pre-Boot Execution Environment (PXE) technology to allow client machines to connect to the server and select an operating system to install. There are notable changes in WDS over RIS including a new graphical user interface used to select the deploy image and the ability to transmit images using multicast. Overall WDS will assist you in reducing the complexity of deployments as well as help to thwart the costs of manual installations across the enterprise.

## Windows Reliability and Performance Monitor

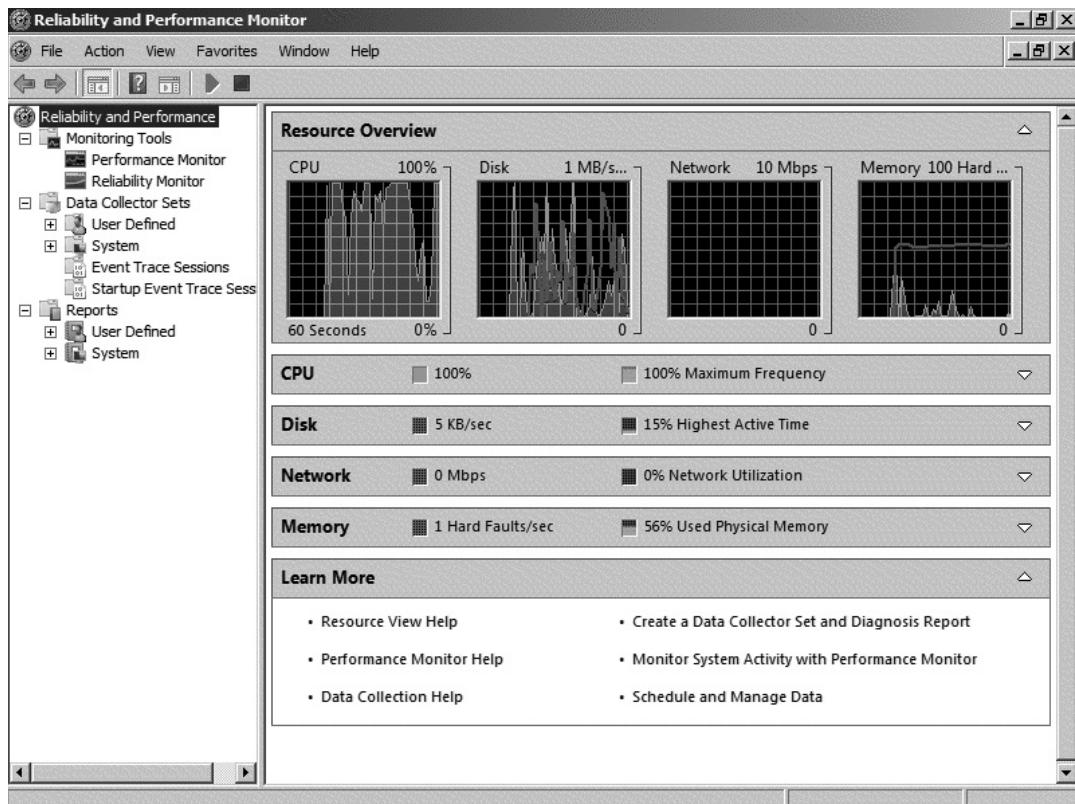
Windows Reliability and Performance Monitor is not to be confused with the Performance Monitor tool. The Performance Monitor tool allows you to utilize counters in order to collect data about local machine resources and services. Both tools exist in Windows Server 2008 and the new tool does take advantage of the same counters that Performance Monitor is based on but it has completely new tricks up its sleeve. It combines the capabilities of Performance Logs and Alerts, Server Performance Advisor, and System Monitor.

The Windows Reliability and Performance Monitor provides a graphical interface for customizing performance data collection and shows real-time data about the status of the server over time. It also contains a Resource View which is similar to functionality previously limited to Task Manager. It allows you to examine real-time information about a machine's CPU, disk, network, and memory usage which can be expanded to display the processed breakdown for each resource.

Reliability Monitor is a component of the tool which calculates a System Stability Index. It accomplishes this by tracking changes to the system and compares them to changes in system stability, providing a graphical view of their relationship. This allows administrators to correlate implementation changes on their servers directly with the problems in performance or stability that may have resulted and

hence create a plan of action to remediate the identified issue. Diagnostics reports can also be generated from the tool (see Figure 2.4).

**Figure 2.4** Windows Reliability and Performance Monitor Tool



With Windows Server 2008 it is plain to see that you have many new tools available for your disposal in order to manage servers in your environment. To best take advantage of the new technology available with Windows Server 2008, taking time to plan out which tools you will utilize and what policies and procedures are to be observed in your server administration and management process would be a good first step!

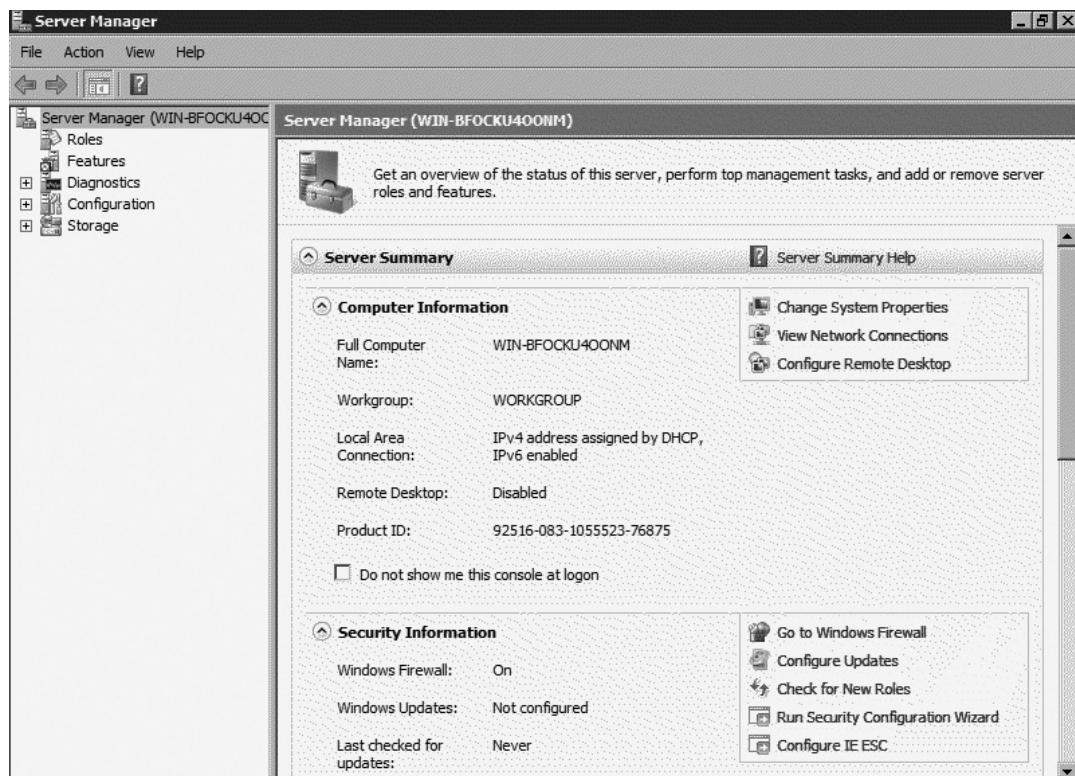
## Server Manager

In the world of IT it can be frustrating to attempt to remember each administrative tool and what its purpose is as well as where to find it in the system. In order to remedy

some of an administrator's complexity and make things easier to use and locate. Microsoft has put together a new tool for Windows Server 2008 called Server Manager. This incarnation is not to be confused with the Windows NT 4.0 version of Server Manager. This new utility slices, dices, washes your car and makes your bed along with doing most of your installation work for you! This single tool gives you the ability to perform heaps of administrative tasks, and all of these tasks are neatly grouped into categories for an easy locating experience. You can Add/Remove Roles, Add/Remove Features, Run Diagnostics, adjust your Configuration, and even manipulate Storage and run Backups on the server.

Upon logon to a Windows Server 2008 the tool automatically starts to assist you with systems management. The main page contains informational data while the tree pane displays the multiple sections where administration can occur. The main page is shown in Figure 2.5. Server Manager has become the new center of installation for Windows Server 2008 and has replaced the Add/Remove Windows Components of previous Windows Server incarnations.

**Figure 2.5** Server Manager Main Console Window



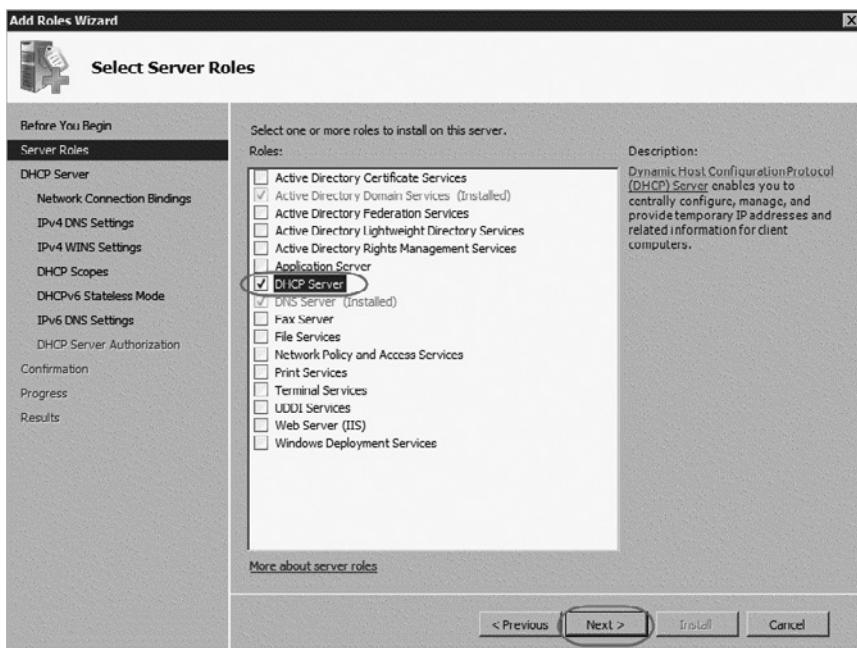
The first tree item in the console is the **Roles** node. In Windows Server 2008, a server role describes the primary function of the server. A single server can have multiple Roles and combining roles should not be performed without some forethought to resource allocation on the server. Some services are processor heavy where as others rely more on memory. Combining services that complement each other in their resource usage is always a good idea. Too many services on a single machine can result in performance problems if the proper planning steps are not taken. To add roles to a server follow the steps detailed in Exercise 2.1.

## EXERCISE 2.1

### ADDING ROLES TO A WINDOWS SERVER 2008

1. Click Start | Server Manager.
1. Select **Roles** from the tree pane.
2. In the details pane in the **Roles** section select **Add Roles**.
3. In the **Before you Begin** page of the **Add Roles Wizard** select **Next**.
4. On the **Select Server Roles** page check the boxes for any roles you would like to add to the server and click **Next** (see Figure 2.6).

Figure 2.6 Adding the DHCP Role to a Windows Server 2008



5. Continue through the **Add Roles Wizard** selecting options as appropriate for the role you have selected.
  6. On the **Confirm Installation Selections** page review your selections and once you are done click **Install**.
  7. On the **Installation Progress** screen wait for your selections to be installed. Once installation has completed the **Installations Results** screen will display.
  8. Review the results for any **Warnings** or **Errors** and then click **Close** to complete the **Add Roles Wizard**.
- 

The next node in the tree is the **Features** node. Some of the **Roles** you install will install **Features** along with them, but most **Features** will need to be installed individually. Some samples of the **Features** available include:

- Network Load Balancing
- Remote Assistance
- SMTP Server
- SNMP Services
- Telnet
- Windows PowerShell

Depending on your needs and the function of the server there may be a few or many Features installed on a given machine.

The third node down the tree is the **Diagnostics** node. Here is where you will find some familiar faces like Event Viewer and Device Manager. Device Manager hasn't learned many new tricks. It functions in Windows Server 2008 most or less as it did in Windows Server 2003. Event Viewer on the other hand has learned some new tricks. Event Viewer now has advanced filtering capabilities. You have the ability to filter by role, as well as by Administrative Events. You can create your own custom filters as before, but the interface has had a new tab added which allows you to edit the filters you create manually (see Figure 2.7). The Diagnostics section is also home to the new **Reliability and Performance** tool discussed previously.

**Figure 2.7** Manually Editing an Event Viewer Filter

The fourth node in the tree is the **Configuration** node. This section is home to some old friends—**Task Scheduler**, **Services**, and **WMI Control**. **Task Scheduler** allows you to schedule tasks to be run at a time that you specify automatically. The **Services** node allows you to view and manager all installed services on the machine and WMI Control gives you access to administrate the WMI service on your server. A welcome addition here is the **Windows Firewall and Advanced Security** section. This allows you a graphical format to configure security and create firewall Inbound and Outbound rules on the machine. Wonderful summary detail exists at the main nodes in the tool and there is also a **Monitoring** section which allows you to see what the system is on the lookout for and its current status. Logging of activity is also performed in the Monitoring section.

The final node in the tree is the **Storage** node. Two main functions exist here: Windows Server Backup and Disk Management. Windows Server Backup must be added as a feature on the machine before you can utilize it. Once it has been added you will see that it has had a total makeover. A new Status and Messages pane have been added and scheduling backups has been simplified drastically. A right-click reveals a **Backup Schedule...** and a **Backup Once...** option easily allowing you to select and run the wizard appropriate for you. **Recover...** and **Configure Performance Settings...** are other choices. The **Disk Management** console on the other hand remains largely unchanged and still serves its main function of allowing you access as administrator to the physical disk on the local machines. One huge new disk feature in Windows Server 2008 is the ability to natively shrink disks. In the past once you had created a partition and presented it to the operating system that space was used for good. Third-party tools do exist on the market that allow you to shrink disks but their results vary and some result in fatal outcome for many servers. Now with Windows Server 2008 and the ability to natively shrink as well as expand disks the ability to restructure your disk architecture on a given server becomes easily do-able.

Server Manager will fast become one of your favorite tools. Since it brings some commonly used tools together and couples them with new and exciting components of Windows Server 2008 is really presents you the best of both worlds – tools you are familiar with that allow you to already do your job effectively, as well as new tools to explore and take advantage of in order to expand your management capabilities.

## ServerManagerCMD

ServerManagerCmd.exe is the command-line counterpart for Server Manager. For those of you who prefer command line or who are handy with scripts this tool will allow you to install and remove roles and features. You can also use ServerManagerCmd.exe to query the server for the list of available roles and features, as well as the ones that are currently installed on the server. For environments where many servers exist, or where most installations processes are performed through automation ServerManagerCmd.exe is a powerful and welcome tool.

Figure 2.8 shows a sample output from a **ServerManagerCmd.exe –query** command.

**Figure 2.8** ServerManagerCmd.exe –query Output

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright <c> 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>servermanagercmd -query
-----
----- Roles -----
[ ] Active Directory Certificate Services [AD-Certificate]
  [ ] Certification Authority [ADCS-Cert-Authority]
  [ ] Certification Authority Web Enrollment [ADCS-Web-Enrollment]
  [ ] Online Responder [ADCS-Online-Cert]
  [ ] Network Device Enrollment Service [ADCS-Device-Enrollment]
[X] Active Directory Domain Services
  [X] Active Directory Domain Controller [ADDS-Domain-Controller]
  [ ] Identity Management for UNIX [ADDS-Identity-Mgmt]
    [ ] Server for Network Information Services [ADDS-NIS]
    [ ] Password Synchronization [ADDS-Password-Sync]
    [ ] Administration Tools [ADDS-IDMU-Tools]
[ ] Active Directory Federation Services
  [ ] Federation Service [ADFS-Federation]
  [ ] Federation Service Proxy [ADFS-Proxy]
  [ ] AD FS Web Agents [ADFS-Web-Agents]
    [ ] Claims-aware Agent [ADFS-Claims]
    [ ] Windows Token-based Agent [ADFS-Windows-Token]
[ ] Active Directory Lightweight Directory Services [ADLDS]
[ ] Active Directory Rights Management Services
  [ ] Active Directory Rights Management Server
  [ ] Identity Federation Support
[ ] Application Server [Application-Server]
  [ ] Application Server Foundation [AS-AppServer-Foundation]
  [ ] Web Server (IIS) Support [AS-Web-Support]
  [ ] COM+ Network Access [AS-Ent-Services]
  [ ] TCP Port Sharing [AS-TCP-Port-Sharing]
  [ ] Windows Process Activation Service Support [AS-WAS-Support]
    [ ] HTTP Activation [AS-HTTP-Activation]
    [ ] Message Queuing Activation [AS-MSMQ-Activation]
    [ ] TCP Activation [AS-TCP-Activation]
    [ ] Named Pipes Activation [AS-Named-Pipes]
  [ ] Distributed Transactions [AS-Dist-Transaction]
    [ ] Incoming Remote Transactions [AS-Incoming-Trans]
    [ ] Outgoing Remote Transactions [AS-Outgoing-Trans]
    [ ] WS-Atomic Transactions [AS-WS-Atomic]
[ ] DHCP Server [DHCP]
[X] DNS Server [DNS]
[ ] Fax Server [Fax]
[ ] File Services
```

## Delegating Administration

Help. Everyone needs some. In the world of IT one of the most effective ways to solicit help is to delegate. Delegation involves assigning tasks or requesting assistance with various tasks to fellow administrators in your organization. They may be your team members, your colleagues, or your employees, but developing a strategy around delegation in your IT world should help to ensure that all people requiring access have it, but a balance must be reached with delegation. Giving too much in the way of permissions to a person opens the doors to potential configuration problems and may create vulnerability in the environment, not enough permission and administrators cannot perform their duties. There are many ways delegation can occur in an

organization and we will discuss the mechanisms pertinent to Server Administration. These include Delegating Authority, Active Directory object delegation, and application management. We will discuss each of these in the next sections. With proper delegation in place administrators at all levels in the environment can successfully and effectively perform their job tasks and in turn help each other out.

## Delegating Authority

In order to grant other administrators permissions in Active Directory there are a few different approaches that can be taken. You can choose to simply make all administrators in your environment a Domain Administrator by adding them to the appropriate group. This however has the effect of giving them the keys to the castle. If their job function involves creating new security groups but never new user accounts by adding them to the Domain Administrators group you have given them permissions above and beyond their limited needs. The better approach to delegation of permissions in Active Directory is to simply grant permissions to administrators based on their job function, thereby limiting their access beyond the scope of their responsibility, hence employing the principle of least privilege.

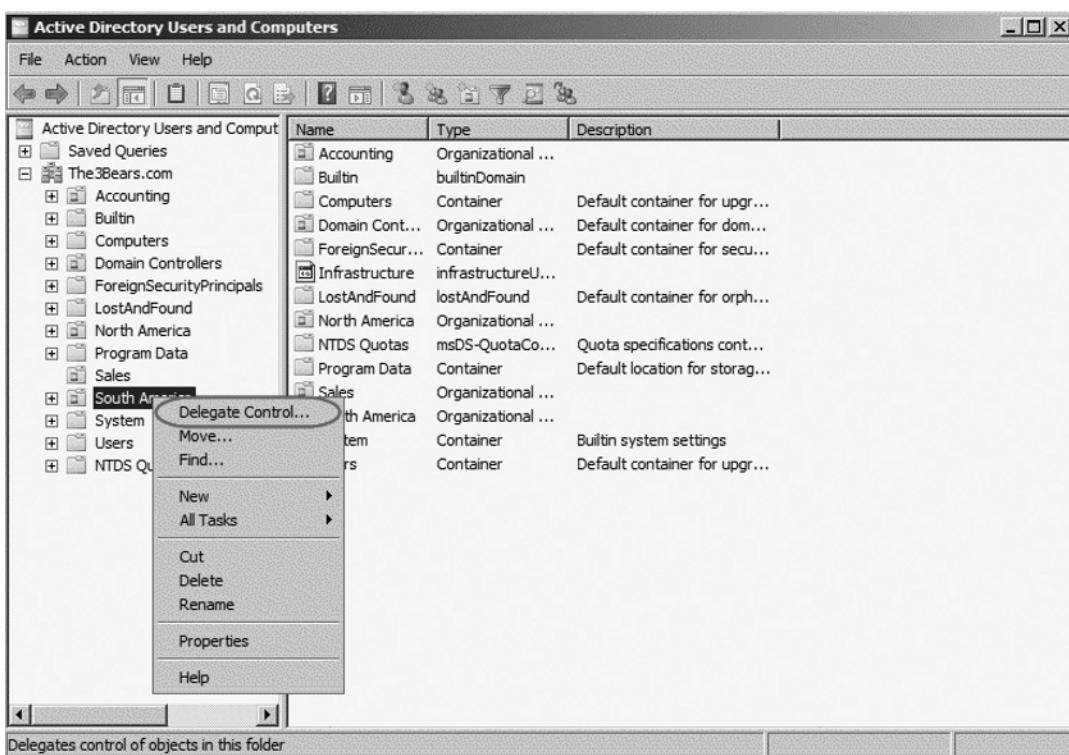
To Delegate Authority in Windows Server 2008 you can take advantage of the built in wizards that exist in the Active Directory Users and Computers console (see Figure 2.9). Typically you would delegate permissions to administrators at the OU level. This allows you to grant rights to administrators over just a certain portion of the Active Directory that is relevant to them. If they are in charge of managing Europe then delegating permissions to the Europe OU is the next logical step. For administrators that need more permission and have wider impact in the environment it may be more desirable to delegate permissions at the domain level rather than at the OU level. Either way the general idea is to grant permissions on the object which intrinsically includes all child items. So for instance, if I were to delegate permissions on the Europe OU to Suzi and the Europe OU contains both users and computers accounts, Suzi's permissions would inherit to both object types by default giving her the ability to administrate both object types.

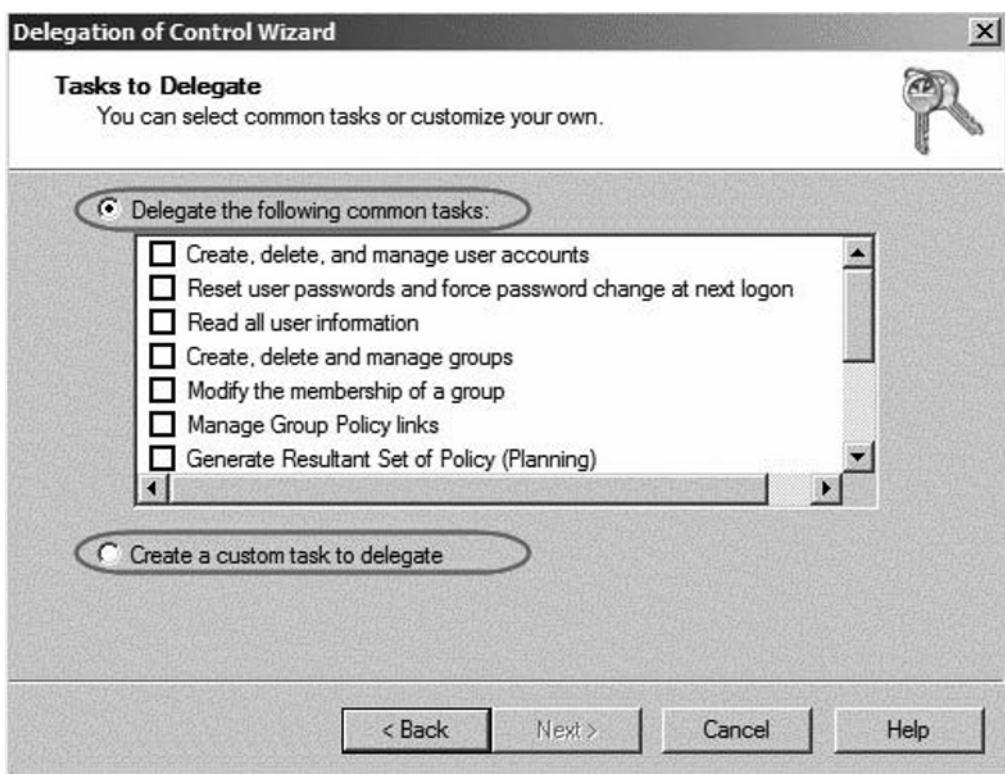
### TEST DAY TIP

 It is always a better choice to delegate permissions to groups rather than to individual users. This allows for ease of administration later when additional user accounts will require the same rights. They can simply be added to the group instead of having to re-run the delegation wizard to grant them rights.

When you run the delegation wizard you must select who will receive the permissions and then where the permissions will apply. The last piece of the puzzle is to determine what permissions they will receive. Microsoft has shrink wrapped certain tasks and made them assignable via the wizard (see Figure 2.10). They are a collection of the more common tasks administrators may perform in Active Directory. If the pre-existing permission sets do not meet your needs you have the ability to customize the permissions you grant to your administrators from within the wizard. Keeping it simple, this cannot be stressed enough. Trying to troubleshoot problems surrounding administration down the road may become challenging if many custom permissions have been applied and not much documentation around it has been created. Keeping it simple is in the best interest of current and future administrators.

**Figure 2.9** Running the Delegation Wizard in Windows Server 2008 Active Directory



**Figure 2.10** Selecting the Permissions to be Delegated

## Delegating Active Directory Objects

Sometimes delegation at the OU or Domain level is just too lenient. If Suzi's job role has her resetting user passwords and updating user account properties she may never have any provocation to administrate computer accounts. In a true application of the principle of least privilege Suzi would simply not need delegated rights on the computer accounts. Active Directory does give you the ability to delegate all the way down to the attribute level if you want to get crazy, but for the need described here delegation at the object level would suffice. So instead of Suzi being granted Modify permissions on the Europe OU, she may only be granted modify on the user objects within the Europe OU, therefore tightening her scope of permissions down to match her scope of responsibility.

## EXERCISE 2.2

### DELEGATING PERMISSIONS ON AN ACTIVE DIRECTORY OBJECT

1. Click Start | All Programs | Administrative Tools | Active Directory Users and Computers.
2. In the Active Directory Users and Computers window expand your domain name.
3. Select the OU you would like to delegation permissions on.
4. Right-click on the OU and select Delegate Control...
5. In the Welcome to the Delegation of Control Wizard screen click Next.
6. On the Users or Groups screen click the Add button and type in the name of the Groups or Users to whom you wish to delegate permissions.
7. Click OK and then click Next.
8. On the Tasks to Delegate screen choose the Create a custom task to delegate radio button and click Next.
9. On the Active Directory Object Type screen select the type of object to wish you would like to delegate permissions for (Entire folder, User, Group Computer Objects, etc.) and then click Next.
10. On the Permissions screen select the permissions you would like to assign (Full Control, Read, Write, etc.) and then click Next.
11. On the Completing Delegation of Control Wizard page click Finish.

## Application Management

In most Windows-based environment applications are traditionally distributed. Each user runs a local copy of all the applications they need to do their jobs. This can make things difficult on administrators in the following ways:

- Upgrades
- Maintenance
- Troubleshooting

When upgrades are required for an application the administrator must push the new version of the software out to all instances of the application in the environment. Testing can be complex since the interaction of the new software must be considered against all possible client installations. Maintenance of applications also presents challenges. Every time routine patches are required a push must take place to all the instances of the application. Sometimes a reboot may be required so there is the issue with scheduling or forcing a reboot once the patches have applied. Also, the administrator must be able to keep track of machines that have and have not received the changes. Since each machine is most likely unique in some way or another troubleshooting can also become complex across a large enterprise. All of these things factored together makes for a rough administrative experience for you when it comes to keeping applications in check in any reasonable sized network.

So what is the solution? In previous incarnations of Windows, Microsoft offered Terminal Services (TS) as a possible option. The TS administrators would centrally install applications on the TS servers and give the users access to run the applications on the server via a Remote Desktop connection. Remote Desktop allows users to connect to the server, log on, and view the local server desktop. From here users could launch any locally installed application to which they had been granted rights. This prevented administrators from having to deploy applications to each client machine in the enterprise. All maintenance, upgrades, and troubleshooting would be performed centrally on the TS servers. The problem presented with traditional Terminal Services is that the Remote Desktop method utilized by the user to gain access to the server based applications gave the user two desktops—their local desktop and the server desktop via the Remote Desktop connection. This configuration created a learning curve problem for most users and required the installation of a user training program, not to mention added help desk calls around the potential confusion with “two” desktops.

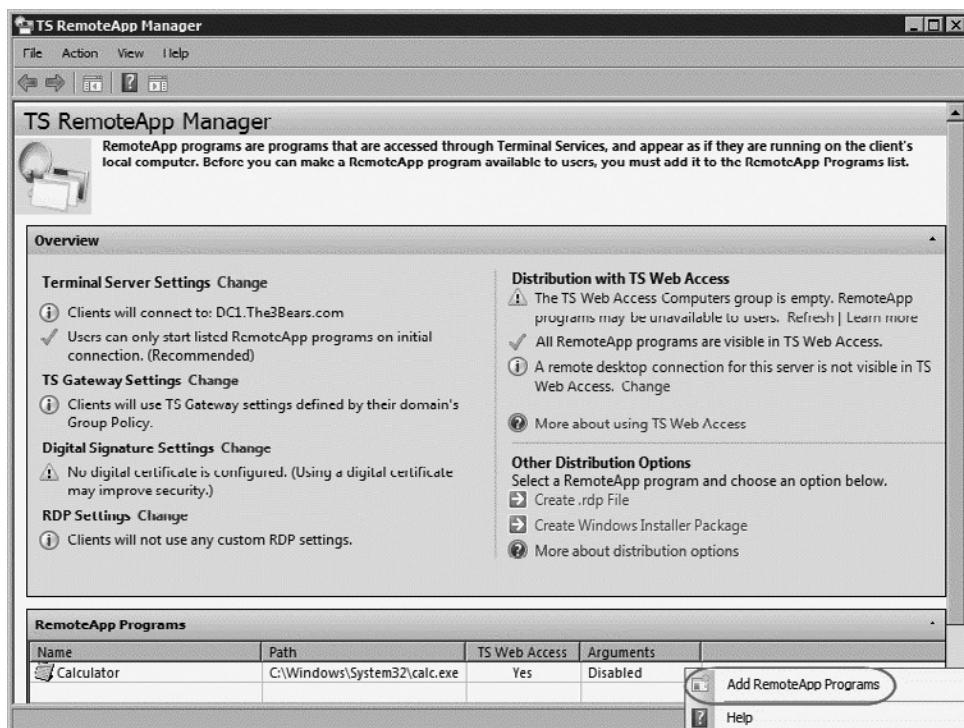
With Windows Server 2008 many of the problems and concerns with centralizing applications are removed. Microsoft has taken their traditional Terminal Services component and added a spin. A new Windows Server 2008 feature called RemoteApp now allows you to share an application through Terminal Services, but only the application is shared as opposed to the server’s entire desktop. The user no longer needs to connect via Remote Desktop and launch applications from the server side desktop. Using RemoteApp the application is launched via a Remote Desktop Protocol (RDP) file. There are three different ways you can make the RDP file available to the user in order to launch the application:

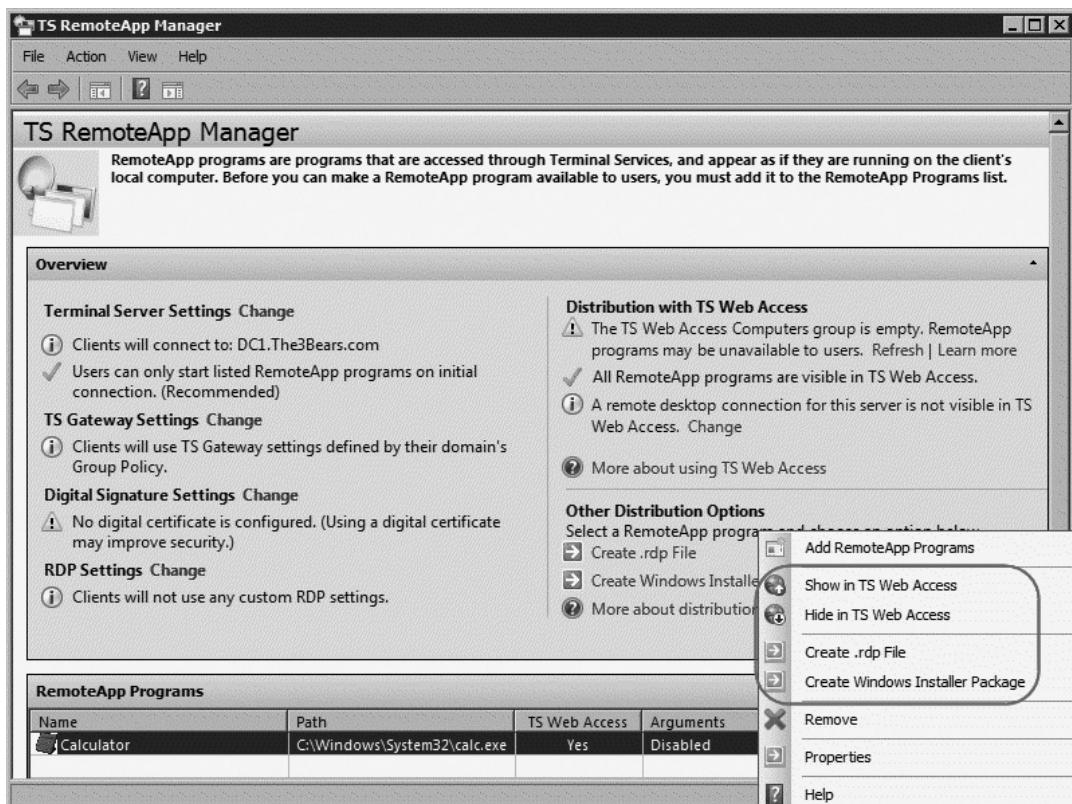
- Traditional Remote Desktop Protocol (RDP) file format
- Group Policy via an MSI file
- Terminal Server Web Access (TSWA)

All three methods present the user with an icon which they simply click to launch the application as they would normally. Even though the application appears as if it is installed locally, unbeknownst to the user the application is actually initiating on the TS backend.

The first step in making any application available to users is to add it to the RemoteApp Programs List on the TS server (see Figure 2.11). Once it is added into the Programs List, you need to decide on the Distribution method for the application. In the RemoteApp Manager Console you can select the application from the RemoteApp Programs list and from the right-click menu you can choose to show the application in TSWA or create an MSI or RDP file (see Figure 2.12).

**Figure 2.11** Adding an Application to the TS RemoteApp Manager Programs List



**Figure 2.12** Selecting a Distribution Method for an Application

Windows Server 2008 adds power and flexibility into Microsoft Terminal Services. It provides administrators the ability to transform what was once tedious and confusing server side desktop launching for centralized application access into what is now simplified icon based server side application launching. By removing the server desktop from the Terminal Services picture in Windows Server 2008 administrators are able to retain the benefit of centralized application management while at the same time reducing the need for specialized user training.

### TEST DAY TIP

With TSWA there is greater flexibility in updating application RDP files. For instance, if new command line arguments become necessary for an application the change can be performed on the TS server without

having to update local RDP files on user machines. Also, since TSWA is accessed through a web browser the RDP files can be made available to domain joined or non-domain joined machines. Group Policies have the restriction of only being able to provide the RDP file to machines in the domain.

---

## EXERCISE 2.3

---

### ENABLING AND ACCESSING AN APPLICATION WITH TSWA

1. Click Start | All Programs | Administrative Tools | Terminal Services | TS RemoteApp Manager.
  2. In the RemoteApp Programs pane right-click and select Add RemoteApp Programs.
  3. On the Welcome screen click Next.
  4. On the Choose programs to add to the RemoteApp Programs list select the checkbox next to Paint and click Next | Finish.
  5. Verify that Paint displays in the RemoteApp Programs pane.
  6. Right-click Paint and select Show in TS Web Access.
  7. Select Start | All Program | Internet Explorer.
  8. In the Address bar type in the following url: <http://localhost/ts> and hit Enter on the keyboard.
  9. On the RemoteAppPrograms tab click on the icon that is displayed to launch Paint.
  10. Provide credentials with membership in the Remote Desktop Users group.
- 

## Planning a Group Policy Strategy

A key component of Active Directory is its ability to centrally manage the experience of these users and computers through the use of Group Policy. By offering a centralized management solution, we can take a majority of the “leg work” out of system administration.

Group Policy makes it possible to perform a number of tasks including:

- Password enforcement
- Auditing
- Software deployment
- Desktop management
- Desktop security

In this section, you will learn about the different types of policies available to you as an administrator, how to create and manage these policies, as well as key design principals, such as GPO hierarchies and GPO troubleshooting concepts.

## Configuring & Implementing...

### Looking Before You Leap... into Group Policy

In any Active Directory environment it can be very tempting to simply push the GO button and just fix what is broken as it occurs and put out fires as they are burning you. By pushing the GO button all the time you become a reactive administrator instead of a proactive one. Being proactive in your environment is important especially when it comes to Group Policy. Without a big picture view on how you can impact the infrastructure with on the fly changes you may end up burning down the house in an effort to put out the fire.

For example, let's assume that a user is having difficulty performing a job function because the Group Policy applied to them is removing their Command Prompt. Due to a recent shift in job function they now require their Command Prompt to perform their duties. So you hop into Active Directory and utilizing permissions exclude them from the policy that is removing the Command Prompt. The user can now do their job and the ticket gets closed. Problem solved, right? Wrong! Without taking the time to delve into the real issue here you may have just caused yourself additional grief down the road. When the new ticket comes in from the same user because his mapped network drives are no longer available or his application icons have disappeared or his wallpaper is blue instead of the

Continued

company logo then don't be too surprised. By being quick to band-aid an issue without taking the time to discover the greater impact of your actions you have in turn caused more problems for both yourself and the user.

So in general, keep it in the back of your mind that when you are planning a Group Policy Strategy it is really that—a strategy. The pieces of a group policy need to fit into the Active Directory infrastructure appropriately in order for the user experience in your network to remain appropriate. By reacting instead of taking the time to be proactive you put yourself and your environment potentially in risk's way.

## Understanding Group Policy

In order to adequately deal with a complex and growing IT world every administrator must make some decisions around Group Policy. They must decide what level of impact policies will have on their infrastructure. Some administrators choose to employ Group Policy to do the bulk of their work and devise a methodology which involves creating new group policies to tackle complex administrative tasks.

For example, if you were the administrator of a 5,000 seat organization, which seems more appealing: logging on to each machine and configuring the background and display settings on all 5,000 systems, or implementing one set of rules—or policy—which included the background and display settings and have it “pushed down” to these machines. How about patch management? Would you prefer to manually walk around a CD or DVD to each workstation to patch systems, or would you rather point machines (via a policy) to an update site, where you have pre-approved these patches?

Sites are another key component of Active Directory administration. Sites are the definition of the physical location of a user or machine. In today's world of work, people tend to work from home, work from the office, and travel to branch offices rather frequently. It may be important to manage each of these scenarios differently. Again, it is much easier to manage these systems from a policy as opposed to individual system management.

## Types of Group Policies

Group Policies allow you, the administrator, the ability to manage users and computers in your Active Directory environment. Being able to enforce settings and configurations in your infrastructure allows you to do everything from dictate lockdown to empower users with simplicity. A wide open infrastructure just doesn't

make sense in today's world of viruses, Trojans, and network attacks. It just makes sense as an administrator to take advantage of Group Policy in order to manage your environment in a centralized fashion with ease and flexibility. There are two types of Group Policy:

- Local Group Policy Objects (LGPOs)
- Non-Local Group Policy Objects (GPOs).

There is a good amount of planning and testing that should go into any Group Policy before it is deployed, but to get started you will need a thorough understanding on the types of group policies. These will be discussed in the next sections in more detail.

## Local Group Policy

Local Group Policies exist on every machine. They are stored on each computer individually and affect the local machine and local users with their settings.

The benefit of Local Group Policies is that if a machine does not belong to a domain there is still a mechanism that can be utilized to lock down the local workstation. In the past only one Local Group Policy could exist per machine, but a new feature of Windows Vista and Windows Server 2008 is the Multiple Local Group Policy (MLGPOs). Traditional LGPOs have two configurable sections: a User Configuration section and a Computer configuration section. MLGPOs further segment the User configuration section to allow configuration based on user role. The new User configurations come in three “flavors”:

- Administrator
- Non-Administrator
- User-specific

Each person in an environment falls into one of two user roles: you are an Administrator, calling the shots and controlling the environment, or a non-administrator, living and working in the environment configured by the Administrator. The Administrator role will include any user account that is part of the local Administrators group. The Non-Administrator role is every other user account on the local machine. Each user will either apply the Administrator or the Non-Administrator policy, but never both. The User-specific configuration allows the Administrator to configure additional settings for any individual user on the local machine. There can still only be one local computer configuration policy per machine, and it will affect all users logging on.

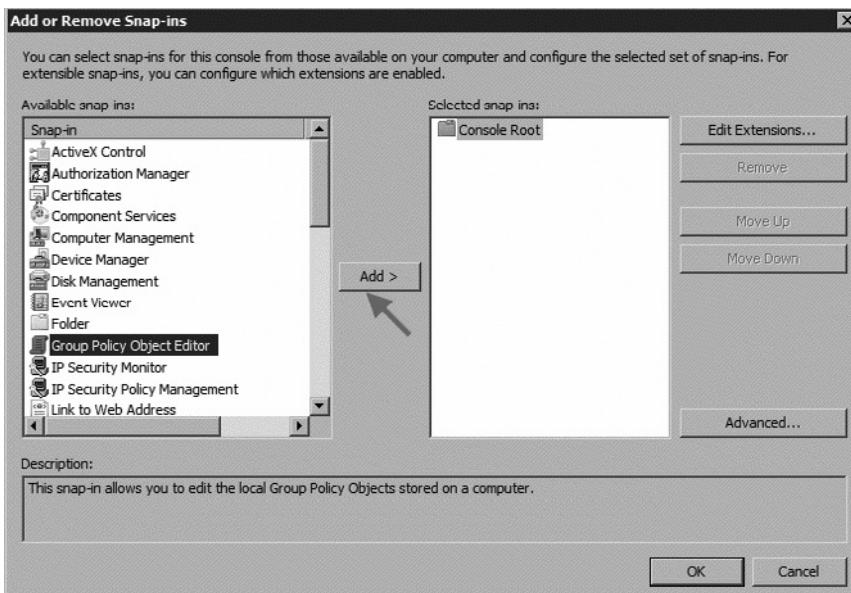
These flavors allow you the flexibility to control users on shared machines, where different types of users may be working on the same workstations throughout the day. This is a particularly useful feature in smaller working environments where sharing is frequent or environments where kiosks and common area machines may be predominant. The one large drawback of utilizing Local Group Policies is that they are configured per machine, so that can become a lot of running around for anyone to manage in larger environments. You cannot edit Multiple Local Group Policies with the default Local Security Policy console from the Administrative Tools menu. The Local Security Policy console allows you to edit the traditional Local Group Policy. You must use a custom console for Multiple Local Group Policies. See Exercise 2.4 for step-by-step detail.

## EXERCISE 2.4

### ACCESSING MULTIPLE LOCAL GROUP POLICIES

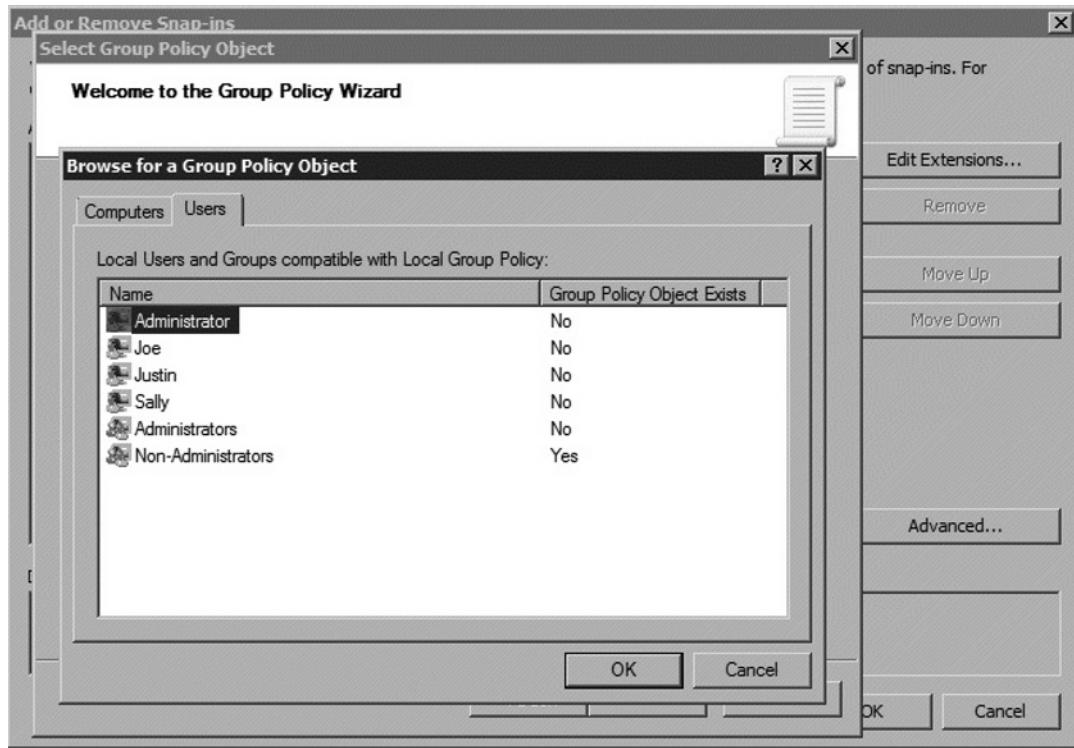
1. Click Start | Run.
2. In the Open dialog box type mmc and click OK.
3. Click File | Add/Remove Snap-in...
4. Then select **Group Policy Object Editor** from the Available Snap-ins: and click Add (see Figure 2.13).

**Figure 2.13** Adding the GPO Editor Snap-In



5. In the **Select Group Policy Object** window click **Browse**.
6. In the **Browse for a Group Policy Object** window select the **Users** tab (see Figure 2.14).

**Figure 2.14** The Browse for a Group Policy Object Window



7. Select **Non-Administrators** and click **OK**.
8. In the **Select Group Policy Object** window click **Finish**.
9. In the **Add or Remove Snap-ins** click **OK**.
10. In the console tree expand the **Console Root**, expand **Local Computer\Non-Administrators Policy**.
11. Expand **User Configuration | Administrative Templates | Control Panel** and click on **Add or Remove Programs**.
12. In the **Settings** pane double-click **Remove Add or Remove Programs**.
13. On the **Setting** tab select **Enabled** and click **OK**.
14. Close all windows and log on as a Non-Administrative account to test the configuration of the policy.

Local Group Policies can be very useful in large and small environments alike. With the new MLPGO user roles workgroups are now offered greater flexibility which contributes to ease of administration. Machines in larger environments that require isolation from the domain can now be locked down more readily as well. Since LGPOs are stored on the local computer, up-keeping the policies and maintaining consistency across machines can prove difficult. Running around machine to machine making LGPO changes is something that can quickly fill an administrator's day.

## Non-Local Group Policy Objects

Non-Local Group Policy Objects exist in the Active Directory with the same purpose as LGPOs—lockdown and configuration. GPOs contain boat loads of settings and configuration options that allow you to depict user and workstation environment in your enterprise. So, for instance, you can perform actions. Machines belonging to an Active Directory domain will download the GPOs affecting them from the Domain Controllers (DCs) in their domain and apply the policy settings. When you create a new GPO in the Active Directory environment it is broken down into a Group Policy Container (GPC) and the Group Policy Template (GPT). The GPC exists in the Active Directory and contains version information and the GPT contains the settings of a policy and is stored in the SYSVOL directory on each DC in the domain. The SYSVOL directory on the DCs is a shared directory which is replicated between DCs. This allows a client to authenticate against any DC and download the policies they require from that same DC. Since the SYSVOL directory is replicated throughout the domain environment the clients receive a consistent copy of any GPO regardless of the DC they connect to. Another benefit in using SYSVOL as a storage location for GPOs is that regardless of where or how many times in AD the GPO is referenced only a single copy of the GPC and GPT needs to be stored. Just like LGPOs all GPOs are divided into two configurable sections:

- User Configuration
- Computer Configuration

These sections each have Policies and Preferences that are configurable. It's the combination of the User and Computer Configuration sections that make up a user's environment on any given workstation in your enterprise.

**EXAM WARNING**

! Know when Group Policies are processed.

Machine starts up:

1. Computer Configurations settings are applied
2. Startup Scripts run

User Logs on:

1. User Configuration settings are applied
2. Logon Scripts run

Background refresh of changes takes place every 90 minutes for both the Computer and the User Configuration. Only changes are applied, not the entire policy.

A command line tool, GPUpdate, can also be used to manually update policies.

---

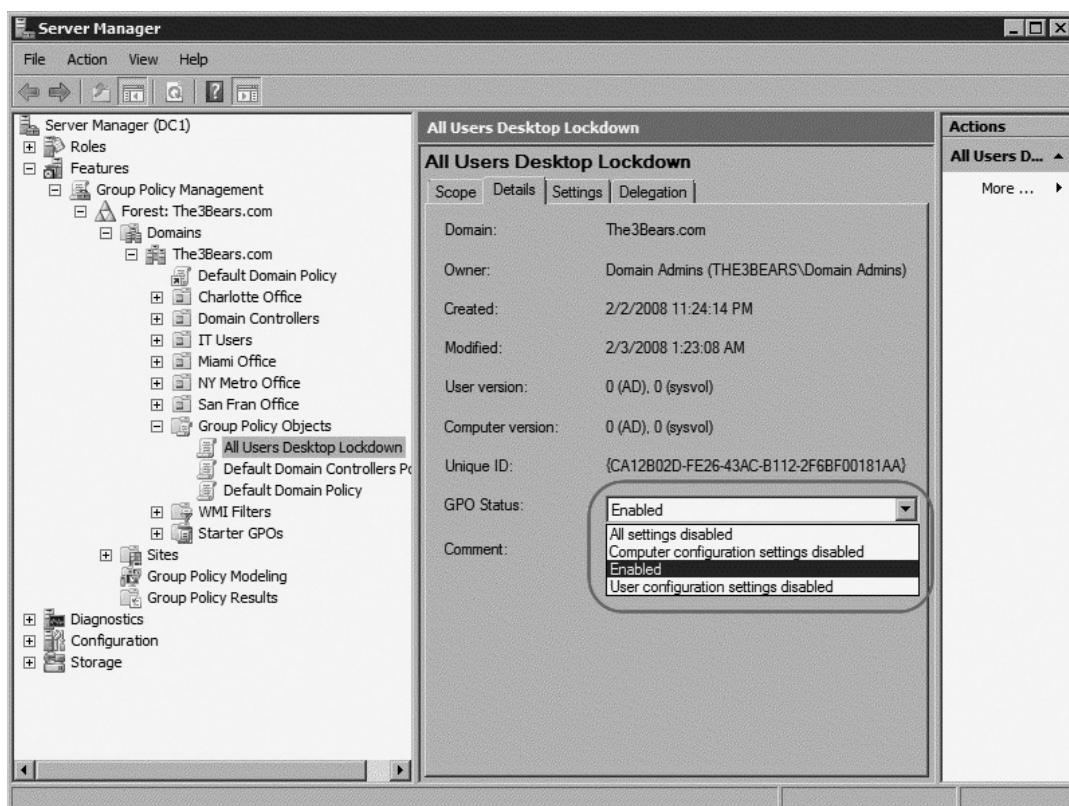
When you are configuring policies you will find occasions when your policy contains only User Configuration settings or contains only Computer Configurations settings, but not both. In these cases it is a best practice recommendation to disable the unused portion of the policy. The benefit of doing so is that downloads will not take place unnecessarily. Normally a computer will download all GPOs applied to it in the Active Directory. The machine isn't aware of how many settings exist in the policy until it actually gets to the GPT and pulls the files and applies them. If the GPT is empty for Computer settings, the machine will be initiating a download without cause. So by disabling policy pieces not in use you ultimately save your machines the trouble of downloading empty policies, as well as unnecessary network bandwidth use.

A policy can also be disabled all together. This is particularly useful when you suspect a policy of causing issues in your environment. You may disable a policy and then test to see if the unwanted effect is gone. If the issue is resolved you know that the policy was the root cause. If the undesired situation persists then you can enable the policy and move on the next one. This allows for easy troubleshooting without having to unlink policies in the Active Directory environment. Perform the following steps to adjust the Status of a policy:

1. Click **Start | Server Manager**.
2. Expand **Features | Group Policy Management | Forest | Domains**.

3. Expand the domain where the policy exists, for example The3Bears.com.
4. Expand **Group Policy Objects**.
5. Select the policy you would like to edit, for example **All Users Desktop Lockdown**.
6. In the center pane click the **Details** tab.
7. Under **GPO Status** click the drop-down menu and select the desired option (see Figure 2.15):
  - Enabled
  - All Settings Disabled
  - User configuration settings disabled
  - Computer configuration settings disabled

**Figure 2.15** Configuring GPO Status Settings





### EXAM WARNING

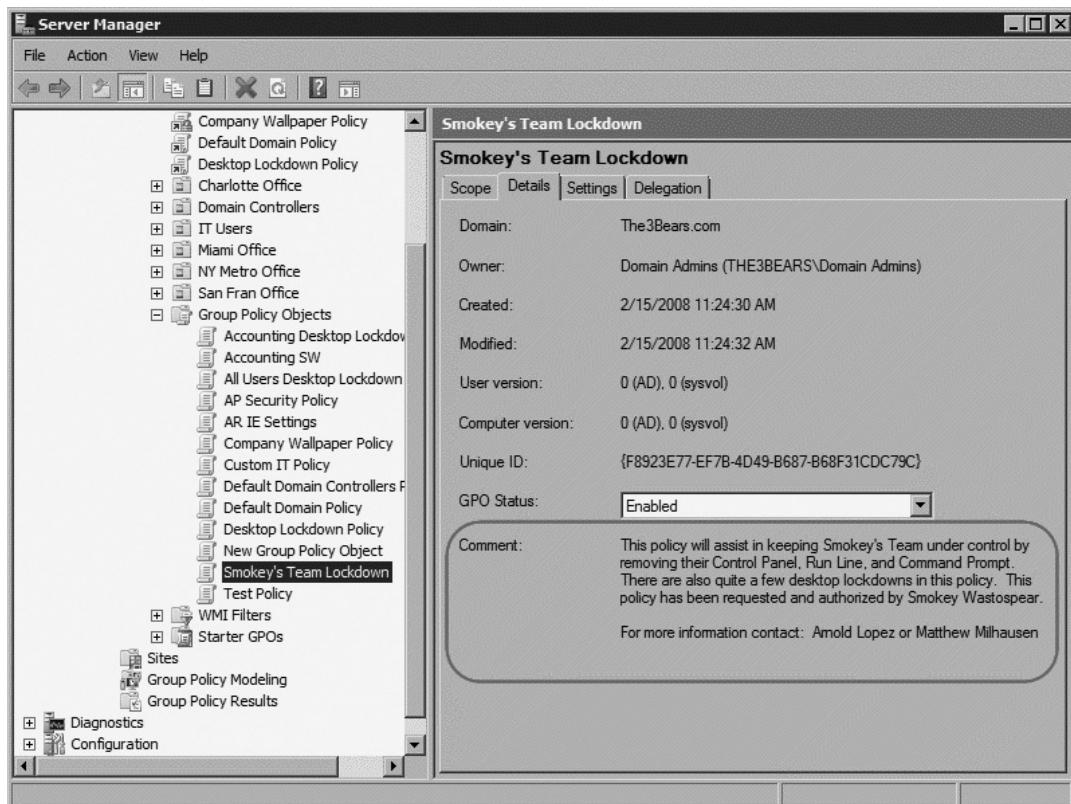
Remember: It is a best practice recommendation to disable unused portions of Group Policies.

As you create policies in your environment it is a good idea to name them in a way that is intuitive. You will find that months later when you return to a policy for whatever reason it will be easier to figure out what was the intended purpose of the policy if you have created a descriptive naming convention and abided by it. To assist in the Administrator's quest for clarity Microsoft has created a new "Comment" section within Group Policy. The Comment section is configured per policy and not per link so each place in the Active Directory where the policy is linked will reflect the same text in the Comment section. The Comment section gives you the opportunity to type in a few descriptive sentences about the Group Policy. You can really input whatever you like, but it may be a good idea to set up company standards around what belongs in this field. Some good suggestions would be to input text describing the author of the policy, who authorized the policy, the purpose of the policy, whom the policy should be affecting and why, etc.

To view the Comment field for a Group Policy follow these steps:

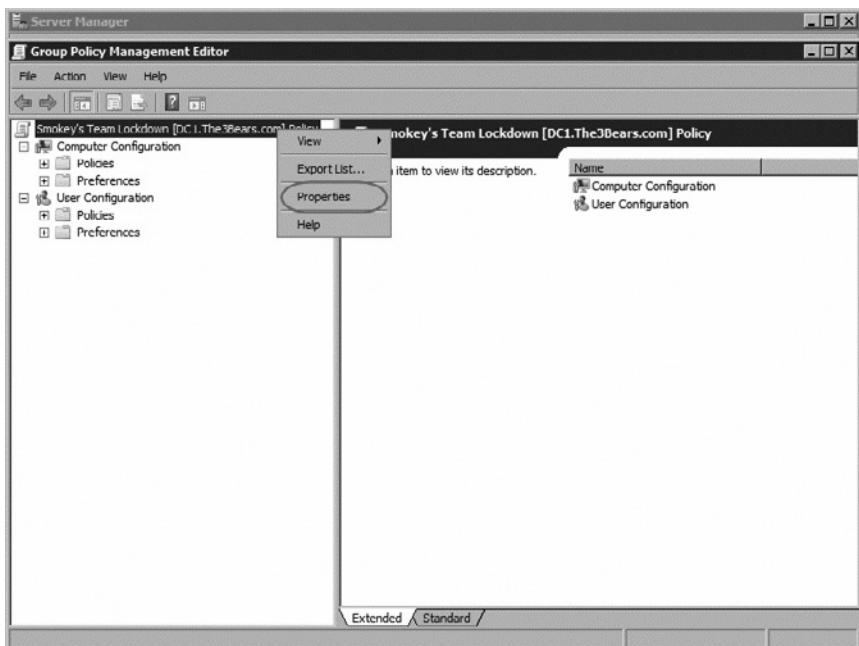
1. Click Start | Server Manager.
2. Expand **Features** | **Group Policy Management** | **Forest** | **Domains**.
3. Expand the domain where the policy exists, for example **The3Bears.com**.
4. Expand **Group Policy Objects**.
5. Select the policy you would like to view, for example **Smokey's Team Lockdown**.
6. In the center pane click the **Details** tab.
7. The **Comment** section is displayed on this tab. See Figure 2.16.

**Figure 2.16 Comment Section of a Group Policy**



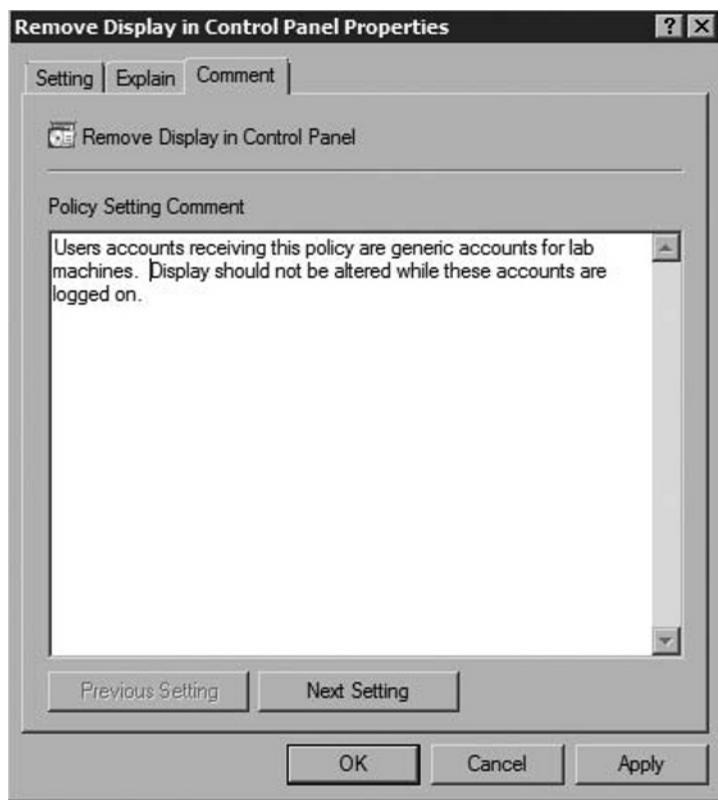
To edit/enter text into the **Comment** field follow these steps:

1. Click **Start | Server Manager**.
2. Expand **Features | Group Policy Management | Forest | Domains**.
3. Expand the domain where the policy exists, for example **The3Bears.com**.
4. Expand **Group Policy Objects**.
5. Select the policy you would like to edit, for example **Smokey's Team Lockdown**.
6. Right click on the policy and select **Edit**.
7. In the **Group Policy Management Edit** window right click the name of the policy and click **Properties**. See Figure 2.17.
8. Select the **Comment** tab to edit/enter text. See Figure 2.18.

**Figure 2.17** Selecting the Properties of a Group Policy**Figure 2.18** Entering or Editing Comments on a Group Policy

The Comment field is also available on each Administrative Template setting within a Group Policy. If there are things you need to remember about a setting, or information that would prove useful to other administrators about how something is configured, a comment at the policy level may be too broad. You can take advantage of the setting level Comment field in order to document additional details. Just remember that the field only exists on Administrative Template settings and will not be visible on Software Settings, Windows Settings, or any Preferences for both User and Computer Configuration. To view the **Comment** tab at the setting levels right-click a setting within a policy and click **Properties**. See Figure 2.19.

**Figure 2.19** Setting Level Comment Field

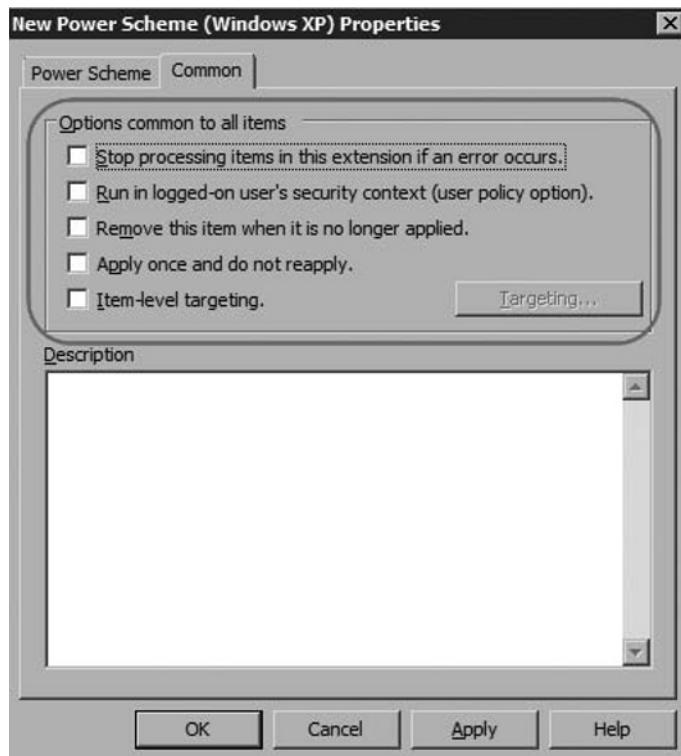


## Preferences

A new feature of Group Policy in Windows Server 2008 is the ability to configure Preferences. Preferences allow you the ability to configure many settings in a user's environment that are not available via traditional Group Policies. Things that were

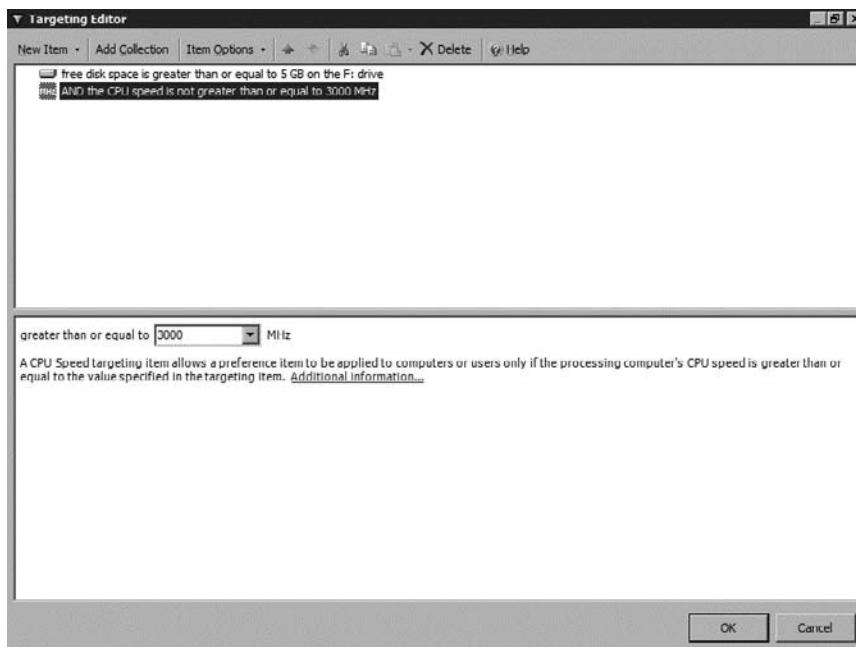
traditionally configured in logon scripts like printers, mapped network drives, and shortcuts can now be set via Preferences. These new settings are extremely interesting in that what you configure is not enforced. When a setting is enforced users cannot change the enforced value and the option to modify the setting will appear grayed out. With Preferences the settings are configured by the policy, however the values are not grayed out and the user can modify the values at any time. For instance, if a user has a shortcut icon created via Preferences, the user retains the ability to edit or delete the shortcut icon. If a policy is removed for any reason the configuration does not revert, but instead it remains as the policy left it. Since the user is not restricted from changing the setting they can edit it at any time. By default Preferences are refreshed when Group Policy refreshes, but this can be configured on a per Preference basis. You can also configure the Preferences in a policy to be applied just once. This can be useful for policies that normally don't require adjustment after their initial configuration, like Environmental Values or Power Settings. Each Preference has a **Common** tab which allows you to configure options (see Figure 2.20).

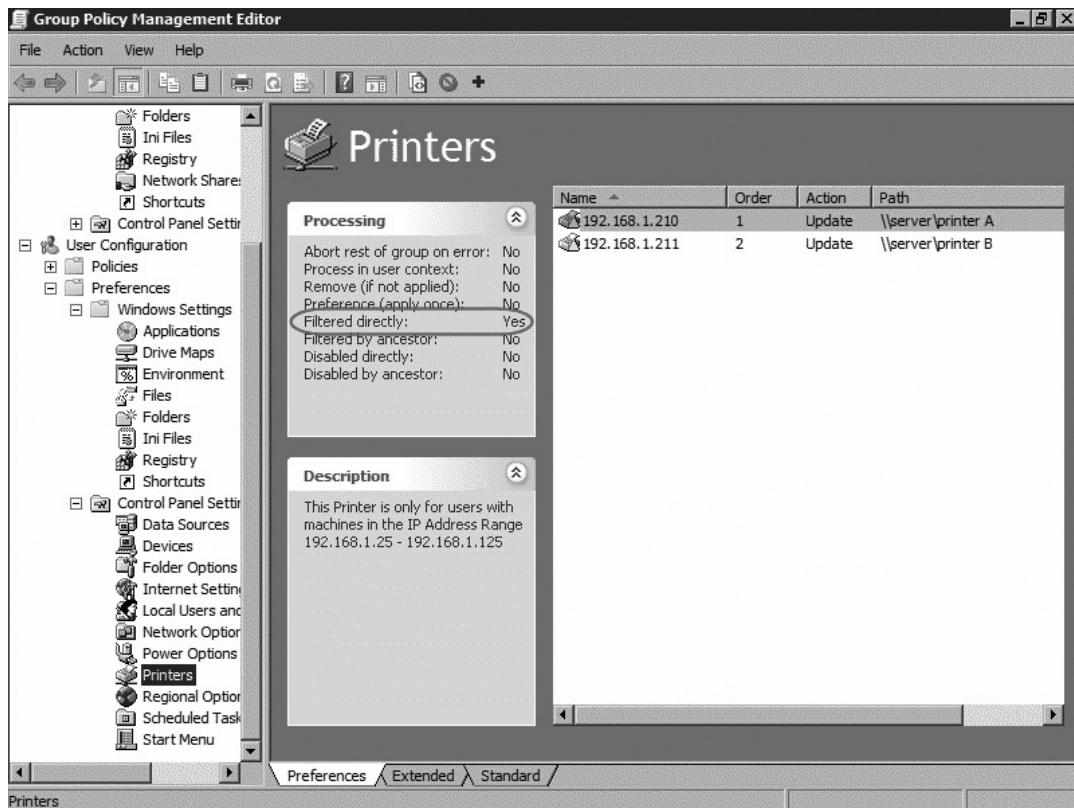
**Figure 2.20** Common Tab Options for Preferences



Another exciting feature of Preferences is the ability to perform Targeting. Targeting allows you to select which users and machines the Preference will apply to. Instead of using mechanisms available in Group Policies like Security Filtering and WMI Filtering, Preferences take things to a new level. Security Filtering uses permissions to allow specific users, computers, and groups to apply a policy. WMI Filtering uses information about the computer like operating system or free disk space to determine if the policy should apply. Both of these mechanisms make a determination as to whether a policy in its entirety should apply or not. So either all the settings in a policy apply, or none of the settings apply. With Preferences there is more flexibility in defining the audience for a policy than with Security Filtering and WMI Filtering. Within Preferences exists a whole slew of criteria that can be combined to target the smallest to the largest groups of users and computers. Settings like CPU Speed, Free Disk Space, Language, IP Address Range, and Operating System are examples of the granularity that can be achieved within the Targeting Editor (see Figure 2.21). Also, Targeting of different groups for different settings can be performed from within a single policy. Since Targeting is configured per Preference setting in a single policy you can have Printer A which pushes to IP Address Range: 192.168.1.25–192.168.1.125 and Printer B which pushes to IP Address Range 192.168.1.126 – 192.168.1.199, as depicted in Figure 2.22.

**Figure 2.21** Targeting Editor



**Figure 2.22** Printer Settings

### **EXAM WARNING**

Group Policy settings are enforced, Preferences are simply set. Users are allowed to modify a Preference after it has been configured on their workstations. If your goal is lockdown then Preferences are not the appropriate mechanism to employ.

### *Network Location Awareness*

In today's disparate world the reality is that users in a large enterprise may be connecting into the domain from a variety of places across a variety of bandwidth types. In situations where the bandwidth may be limited there are certain policies settings that you would not want traversing the wire. Software Policies are a good example

of a group policy setting that just doesn't work in low bandwidth situations. Office 2007 installing across a T1 line to 40 users in a satellite office should only ever occur in an administrator's nightmare—not on their network.

To allow Group Policy to determine what types of settings are appropriate based on the bandwidth of the connected user Microsoft has built a new feature into Windows Vista and Windows Server 2008 called Network Location Awareness. In previous operating systems network bandwidth was detected utilizing the ICMP protocol. Essentially ping packets sent across the network would determine if a connection was deemed “slow” or not. This proved to be a less than perfect solution since in many situations users connecting from a slow link location may have a firewall between them and the domain controller, potentially blocking the ICMP traffic. This prevented proper detection of network bandwidth therefore causing policies to process improperly—allowing for large policy settings to process across slow links. Network Location Awareness mitigates this by making Group Policy aware of the network bandwidth and state.

Earlier versions of Windows Group Policy just weren't aware of the state of the network connection on a machine. Policies apply during system boot, during user logon, and thereafter at regular refresh intervals—that's it. So if a machine were to miss a Group Policy refresh because it was disconnected from the network it would start the countdown timer to the next refresh timeframe. If the machine was reconnected to the network before reaching the refresh interval it would just continue to wait until the refresh time arrives. Group Policy had no indication that the network was now available and that the policies would process successfully. With Windows Vista and Windows Server 2008 the implementation of Network Location Awareness allows Group Policy to become more in tune with the machine's network state. For instance, if a mobile user moves their laptop in and out of different network conditions such as wireless, docked, VPN connected, wired, etc., the processing of Group Policy can occur with each change. So if the machine failed on its last attempt to refresh or if the retry window has arrived then the machine will use the availability of the DCs as an additional factor in determining if Group Policy processing should occur.

## User

Each GPO is broken down into two main components: User Configuration and Computer Configuration. The User configuration has both Policies and Preferences available. The User configuration can be used to do many things including but not limited to deploying software, locking down application settings, administrating desktop settings, and assigning logon scripts. Configuring the user portion of a

GPO gives you the ability to influence a user and their experience, even as they move around within the organization.

For example: Steve arrives at the office, rushes into the nearest conference room, and powers up his laptop. He logs onto the domain to prepare for a conference call. When Steve authenticates against the domain from his laptop all policies affecting his user account in the domain are processed and applied. So let's say that Steve's user account has the following settings in effect from those policies:

- Run line removed from the Start menu
- Control Panel hidden

He finishes his conference call and heads to his desk to officially start the day. He sits at his desk and logs on to the domain again, this time from his desktop machine. Steve is now using a different machine; however, the policies affecting his user account in the Active Directory remain the same. If the summation of the processed policies gives him the settings listed above at his laptop, then from his desktop they would be the same. The policies follow his user account throughout the environment.

## Computer

The computer configuration section of a GPO also has both Policies and Preference sections available. Many of the sections in a GPO overlap between the User and Computer Configuration. Examples of overlap are Scripts, Security Settings, and Control Panel. The contents of each section will vary between User and Computer Configuration and what is possible in one may not exist in the other. The Control Panel settings are a good example of this. There are only two subsections within Control Panel for the Computer Configuration: Regional and Language Options and User Accounts. Control Panel under the User Configuration has much more to offer: Add or Remove Programs, Display, Printers, Programs, and Regional and Language Options. Notice the overlap between Regional and Language Options in the two sections. For the most part setting options in the User and Computer configurations will be different but in the event of overlap a conflict may occur. If a conflict arises between user and computer, the Computer Configuration will take precedence.

There are some settings within Group Policy that can only be applied to a machine. Loopback Processing mode setting is a good example of this. Computer configuration settings can be extremely useful in situations where the user is irrelevant in the application of the policy. Windows Updates and Event Viewer

are good examples of this since regardless of the user logging onto the machine the settings will rarely differ. It just makes sense to apply these types of policy settings to machine accounts rather than user accounts since the logged-on user is irrelevant. Computers that have special function in an organization are also a practical target for computer-based policy settings, such as a dedicated Kiosk machine or a public Web access workstation. In any case Computer Configuration settings can offer a powerful solution to administrators seeking a method of applying machine-based settings across the enterprise.

The desired outcome of the GPO will dictate whether using a Computer settings or User settings would be the appropriate choice. For example, if you worked in a university setting you may want to push a certain software package to all machines on the campus library. If the software package is not appropriate on other computers in the organization, such as student center machines or dorm room machines, then using a Computer policy setting would allow you to configure the software package to apply only to the designated library machines, regardless of the logged-on user account. The user account logging on to the library machines would not impact the software package since it was applied through a Computer policy setting. The same software package assigned as a user setting would yield entirely different results. Software packages assigned to user accounts will either install or become available for install, depending on the package settings in the GPO, on any machine that the user account is able to logon to.

## Planning for GPOs

Without proper planning unexpected results may surface in your Active Directory environment. Since there is a direct correlation between where a GPO is linked in the AD structure and which users or computer accounts it affects it is important for administrators to be aware of the potential outcome of their actions. When applying GPOs in an Active Directory environment it is just as important to take heed of where you are applying a policy as it is to plan what you are putting in it. The default nature of GPOs is to trickle down the tree structure from where it is applied and impact all objects along the way. Without careful planning and consideration you run the risk of ending up with an undesired outcome. As a result of poor planning or a lack of understanding of the AD hierarchy, multiple policies can combine and produce lockdown when it is undesired or allow users to retain settings that may be considered a risk. In order to plan for and deploy an effective Group Policy Infrastructure it is crucial to understand how the AD hierarchy comes into play.

## Site, Domain, and OU Hierarchy

The first policy to process is always the local policy (LGPO). Once the local policy has completed processing, the domain level policies are applied next. Group Policies can be applied at three levels within the Active Directory environment:

- Site
- Domain
- Organizational Unit (OU)

A single GPO can be applied at multiple locations in the hierarchy and any level can have multiple policies applied.

The Site level represents the highest level in which a GPO can be applied. Policies linked at the Site level are the first domain-based policies to be downloaded and applied. Since machines become members of Sites based on their IP address, machines from multiple domains may become members of a single Site. This can present issues since GPOs are stored at the domain level. Only DCs from the domain in which a GPO was created will have a copy of the GPT available for download. If a GPO is created directly on a site object the GPT will be stored in the domain identified as the forest root. Machines may be required to transverse bandwidth to download the pertinent GPO while their users wait. In general linking at the Site should be performed with caution. It has the implication of targeting multiple domains as well as the chance of creating inconsistency for mobile users unless applied with careful planning. With the proper planning and testing linking at the site level can be useful in situations like software deployment, but understanding the ramifications of site linking is critical for you to effectively apply GPOs.

### Configuring & Implementing...

#### Applying GPOs at the Site Level

The Site level may present an unpredictability factor for applying GPOs. The definition of a Site is a group of well-connected computers. You create a Site within Active Directory and then associate it with any subnets that

**Continued**

are considered well connected. Geographically distributed environments will have numerous sites. Users in today's world are mobile and they may move between different Sites by visiting remote offices or in some cases by simply carrying their laptops from building to building on a company campus. Each time a machine moves to a new Site it will be affected by the GPOs linked to the Site it is in at that point in time, hence the unpredictability factor. Sometimes it may get a setting and sometimes it may not—depending on the Site they happen to be in that day. If GPOs linked at the Site level are different from Site to Site the GPO result for a given user or computer will vary. Without knowing which Site a mobile user may be associated with there is no way to consistently enforce policy. However, Site Level policies can be extremely useful if employed properly. Group Policy has certain components, such as Application Distribution and WSUS settings, where site restriction is preferred. You would not want Office 2007 to install across a T1 to a machine sitting in a remote site. In order to prevent these types of occurrences Site Level policies can be leveraged to keep software deployments and other such settings site local.

Once the local and site level policies have been processed the next policies to apply are any Domain linked policies. When applying a group policy at the Domain level the settings configured in the policy will be inherited down the tree structure and be applied to all objects in the hierarchy. This includes both computer objects and user objects in the tree. Applying policies at the Domain level are appropriate when the settings are applicable across the enterprise. Settings mandated by corporate security policies are a good example of a compelling domain level group policy. Since domain level group policies are so wide spread, they will have a large impact if many policies are applied at this level. Keeping domain level policies to a minimum is in your best interest in order to minimize processing overhead.

### **EXAM WARNING**

Remember that one policy with many settings will process faster than multiple policies with few settings each. Reducing the number of policies will speed up the time it takes for policies to download, in turn making logon for users faster.

The final level in the hierarchy is the Organization Unit (OU). In most organizations you will want to apply your policies at the OU level. You will have

more granular control at this tier and the scope of the policy is narrowed to only affect the desired user or computer accounts. The default nature of policies at the OU level is to inherit down the tree structure to all child objects, user accounts, computer accounts, and child OUs and their child objects included.



### TEST DAY TIP

---

In order to assist you in remembering the policy inheritance order take advantage of the paper they will give you during your test. When you first sit down draw the hierarchy of Site, Domain, and OU, you can then reference your diagram as you need it in the questions.

---

## Group Policy Processing Priority

When a machine boots up or a user logs on, the machine is tasked with scrambling to collect and download all applicable policies and applying them in the correct order. The policies that affect a single user or machine can be many and when more than one GPO is applied the end result is a summation of all the policies involved. The end result is similar to a person getting ready to go outside on a cold winter day. Let's say Justin pulls on a long sleeve shirt, a sweater, and finally a jacket. Justin now has different layers of attire that exist; however, the ones underneath are covered up by the pieces put on afterwards. Policies are applied in a similar fashion. Starting from the top of the hierarchy the settings are cumulated, however, if a conflict occurs the last value processed for that setting applies.

The first policy to be applied is the local policy. If the machine is a Windows Vista or Windows Server 2008 (non-Domain Controller) the MLGPO is applied in the following way:

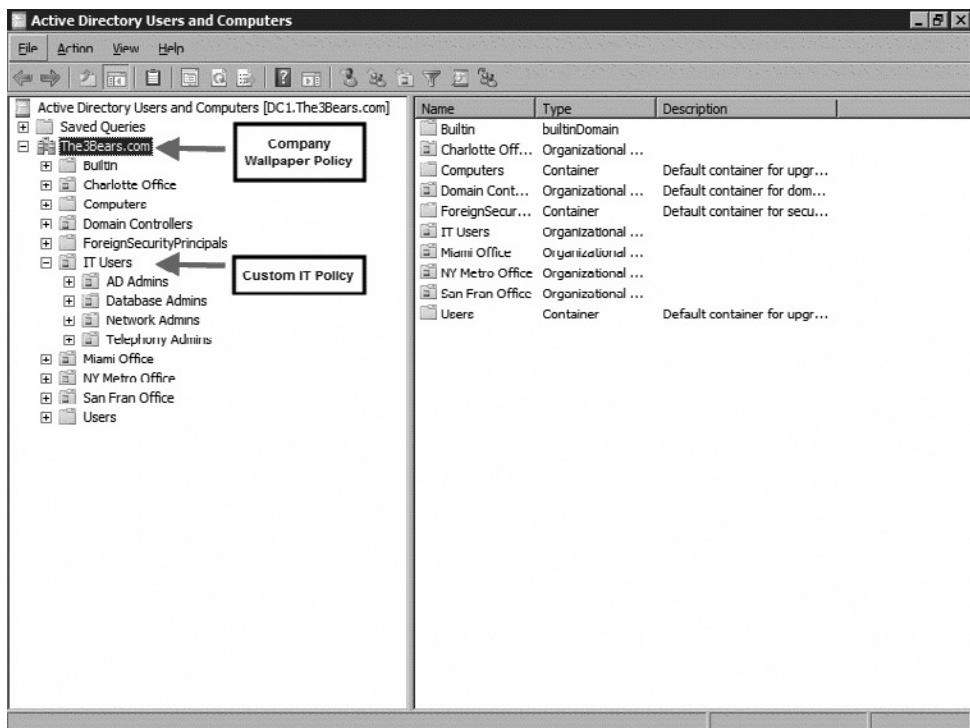
- Local Computer Policy
- Administrators or non-administrators Local Group Policy
- User-specific Local Group Policy

The final policy processed will win in the event of a conflict, so a User-specific setting will always win over a Local Computer Policy setting. Next to be processed are policies linked to the Site level. It is typically not a recommended practice to link GPOs at the Site level. It can be difficult to predict which users will be affected by a Site level policy and when. For example, if a laptop user were to work in the Atlanta, GA office on a Monday, then hop a plane on Tuesday to the Miami, Florida

office to work for the rest of the week the policies that are applied to his machine may differ between the two locations when Site level policies are in use. So if the Miami, FL administrator chooses to lock down the command prompt in a GPO and then applied the GPO to the Miami Site, a programmer visiting that office may lose the ability to perform his job function due to the Site Level policy.

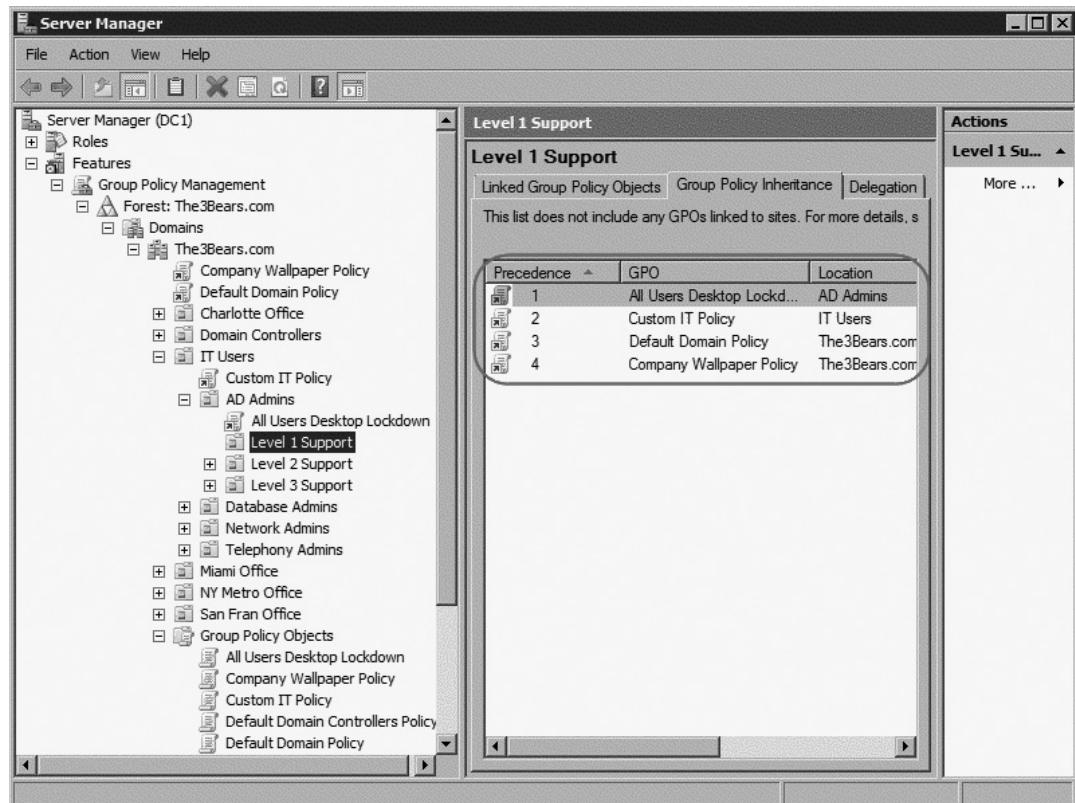
In order to keep things consistent it may be a good idea for you to use caution when linking GPOs with certain settings at the Site level. Once Site Level policies have processed, the next policy to apply are any Domain level GPOs. Finally OU level GPOs will apply. OU level GPOs will transmit their settings to all child objects. So with OU policies depending how deep a user or computer is in the hierarchy they may have many OU level GPOs to apply. The last setting of a policy always wins regardless of where in the hierarchy it originated. In the following image the **IT Users** OU is inheriting one policy and the **Company Wallpaper Policy** has another applied, the **Custom IT Policy** (see Figure 2.23). For a user or computer account residing in the **IT Users** OU the wallpaper setting of **Disable** will apply since the policies on the lower OU will be processed after the Domain level policy.

**Figure 2.23** Inheritance Example



In Figure 2.24 you will see the **Group Policy Management** console displaying the **Group Policy Inheritance** tab for the Level 1 Support OU. The policies listed originated from higher up in the tree structure and are being inherited. Notice that the **Precedence** column lists the **All Users Desktop Lockdown** first, indicating that its settings will override any settings that conflict in the other policies.

**Figure 2.24 GPMC Displaying Inheritance at the OU Level**



## Creating and Linking Group Policy Objects

In order to utilize Group Policy Objects (GPOs) you must first become acquainted with how to create them in your Active Directory environment. You have multiple options in how to go about creating and linking GPOs to containers in your environment. In this section we will discuss:

- Creating Stand-alone GPOs
- Linking GPOs
- Creating and Linking GPOs at One Time

## Creating Stand-Alone GPOs

When you are creating a GPO for the first time, it may be a little worrying to think of the impact you may have if the GPO were to be applied with either the wrong settings or at the wrong place within Active Directory. To avoid any “whoops” that may take place around GPO creation, Microsoft allows you the ability to create stand-alone GPOs. Just as the name implies they are not linked anywhere in the infrastructure upon creation. They are simply floating within your Active Directory universe. Just like any other GPO, stand-alone GPOs will have a GPT and GPC and the settings will exist in SYSVOL for users and computers to download, with one major difference: no one will be downloading them. Since the policies are not linked anywhere in the AD environment users and computers alike will not know that they exist and therefore any changes you make to the policies will go unprocessed. To create a Stand-alone GPO use the following steps:

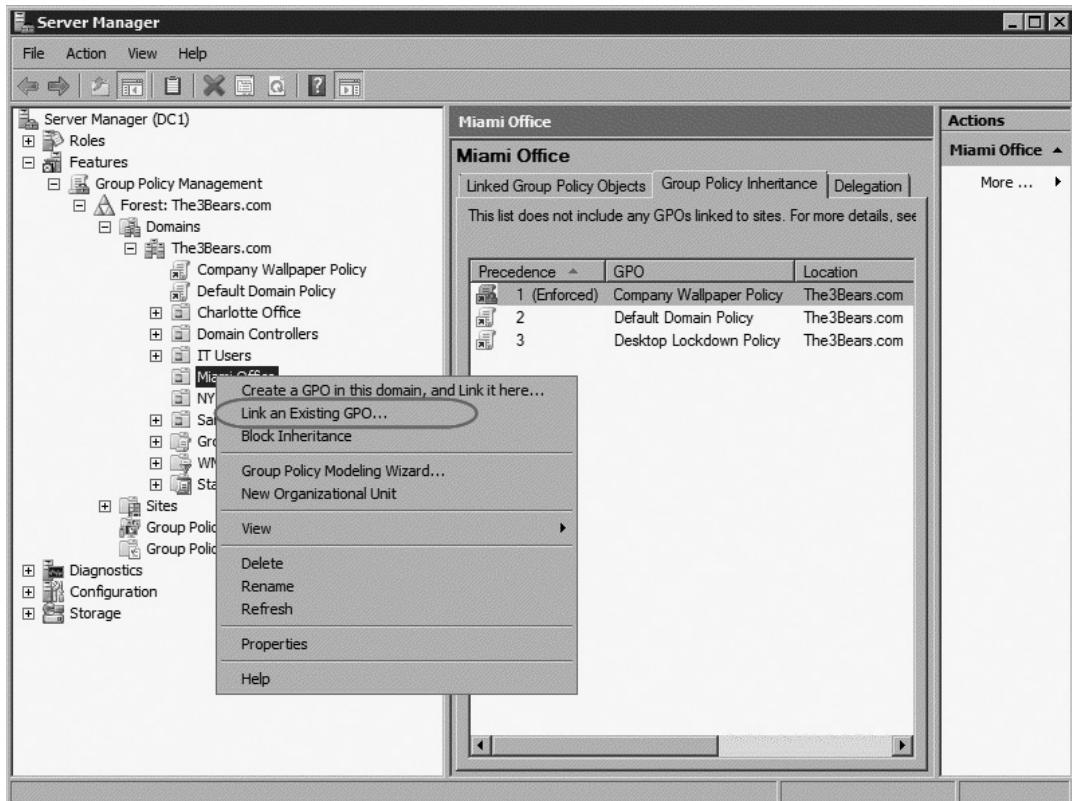
1. Click **Start | Server Manager**.
2. Expand **Features | Group Policy Management | Forest | Domains**.
3. Expand the domain name, for example **The3Bears.com**.
4. Right-click on the **Group Policy Objects** folder and select **New**.

## Linking Existing GPOs

Once you have created a Stand-alone GPO it will affect no person or machine in your environment. In order to have your new policy have an impact on your network you must link it somewhere in the hierarchy. This can be done at the Site, Domain, or OU Level. One of the fabulous things about GPOs is their reusability. So if your Accounting department has incurred administrative wrath and is locked down from toes to chin with Desktop Policies, there isn't any reason why you can't easily spread the joy to the Human Resources Staff if they get on your nerves with the same policy. Once you have created GPOs in your Active Directory environment you may link them at different places within your AD infrastructure with just a few simple clicks. Depending on the design of your AD OU structure you may want to link a GPO to multiple OUs in order to effectively target all the users the policy was designed for. To Link an existing GPO use the following steps:

1. Click **Start | Server Manager**.
2. Expand **Features | Group Policy Management | Forest | Domains**.
3. Expand the domain name, for example **The3Bears.com**.
4. Right-click the location you would like to Link the policy and select **Link an Existing GPO...** (see Figure 2.25).

**Figure 2.25** Linking an Existing GPO

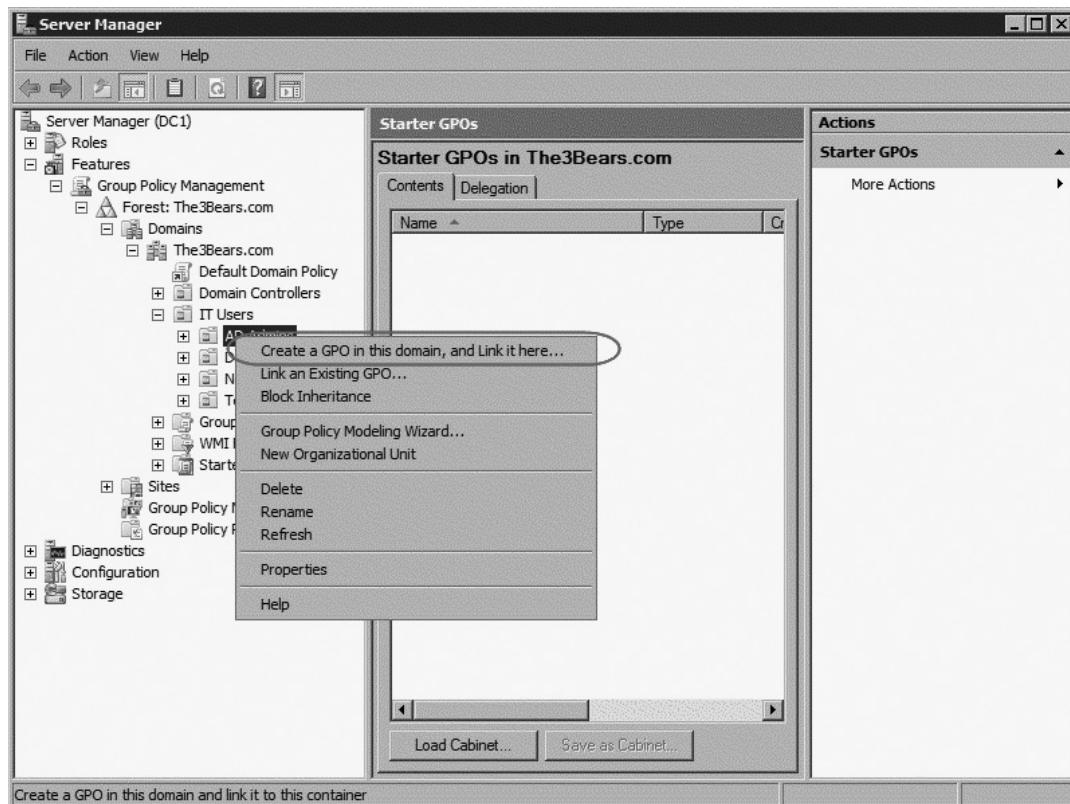


5. In the **Select GPO** dialog box under the **Group Policy Objects** section highlight the GPO you wish to link.
6. Click **OK**.

## Creating and Linking at One Time

In some instances you already know where you would like a GPO to go before you begin creation. In these cases it makes sense to simply create the policy where it is going to be linked and then configure the settings afterwards (see Figure 2.26).

**Figure 2.26** Creating and Linking a GPO with One Action



For step-by-step create-and-link instructions see Exercise 2.5.

## EXERCISE 2.5

### CREATING AND LINKING A GPO

1. Click Start | Server Manager.
2. Expand Features | Group Policy Management | Forest | Domains.

3. Expand the domain name, for example **The3Bears.com**.
  4. Right-click the location you would like to create and link the GPO. In this case the **AD Admins OU**.
  5. Select **Create a GPO in this Domain, and Link it here...**
  6. In the **New GPO** window type in a name for the new GPO. You may also select a **Source Started GPO** in this window if you would like.
  7. Click **OK**.
- 



### TEST DAY TIP

Don't get caught up in the details. Reading too much into an exam question can lead you to draw false conclusions. Take the information in the questions at face value, and remember—you know this stuff!

---

## Controlling Application of Group Policies

In every universe there is the “exception to the rule.” In the case of group policies it isn’t a platypus or a tomato. It tends to be VPs of Finance or the CFO’s secretary or sometimes even your boss and colleagues. No matter the “why” behind the need for an exception, there are a few different mechanisms available to you to tweak and adjust your policies so that everyone can be happy in your environment. Well, within reason anyway.

Being able to bend the rules around policy application can be a fabulous tool when exceptions crop up in your environment. Since group policies will naturally flow down the Active Directory tree structure, altering that flow with Block Inheritance is one way to change the outcome of inherited settings. Another method is to give certain policies preference over others via Enforce. Other mechanisms include Security and WMI Filtering as well as Group Policy Loopback settings. We will discuss each of these in more detail in the following sections.

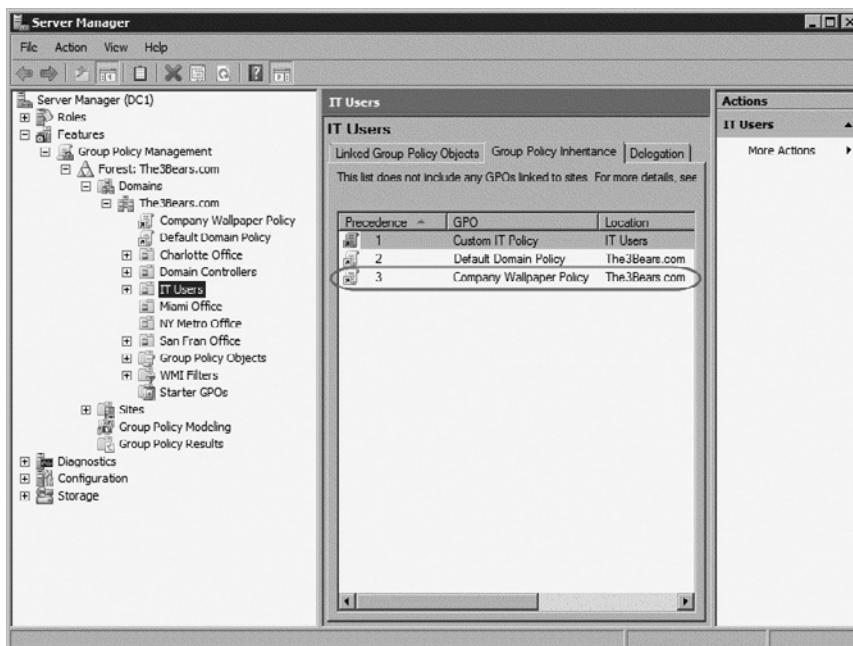
## Enforce

In some organizations certain policies must be applied to everyone in the enterprise, period. Sometimes it's a security mandate that requires all users to have the Run line removed from their Start menus, other times a marketing mandate

that requires all users to have the company wallpaper set at all times, or a legal requirement to display a disclaimer every time a user logs on. The nature of Group Policy inheritance and the hierarchy of Active Directory can sometimes create unfavorable conditions, causing a policy to fail to apply where it is required. Enforce is configured in the Active Directory where a GPO is linked, not on the overall policy itself. So there is the potential to have a policy linked at many different levels but only to have it Enforced where you indicate. The direct effect of Enforce can be seen in the Group Policy Management console.

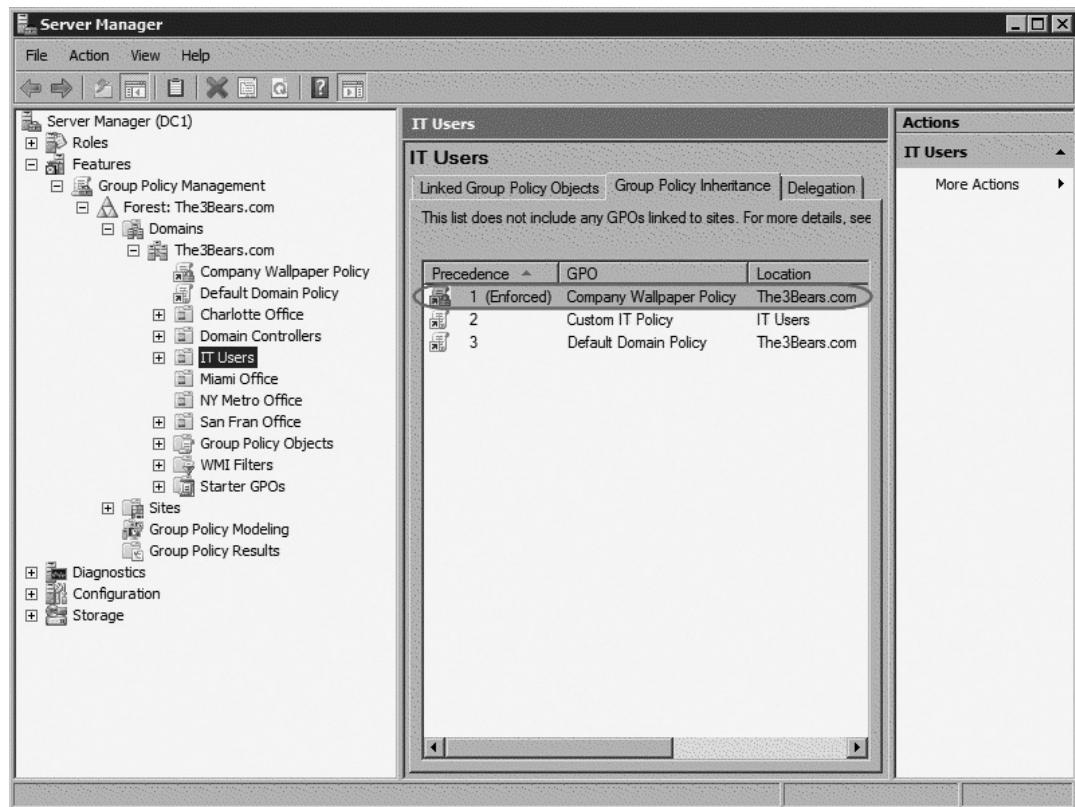
To prevent a mandated policy from being overridden you must mark the link as Enforced. This allows you to avoid the unpleasant situation of having to explain why the marketing manager noticed two employees in the IT department with World of Warcraft wallpaper instead of the prescribed company logo. By giving a wallpaper policy the ability to trample on any and all policies in its way you will save yourself the reprimand. Enforce essentially creates a policy whose settings will “Always win” in the case of a conflict. Notice the policies in Figure 2.27; since all policies are inheriting normally the domain level policy which is named **Company Wallpaper Policy** is at the bottom of the precedence list. This policy has the potential to have the wallpaper setting it is configured with overwritten by both the **Default Domain Policy** and the **Custom IT Policy**.

**Figure 2.27 Normal Inheritance**



By enabling **Enforce** on the **Company Wallpaper Policy** the precedence is directly impacted and now the **Company Wallpaper Policy** moves to the top of the list. At this point it will not be overridden by any of the lower precedence policies. See Figure 2.28.

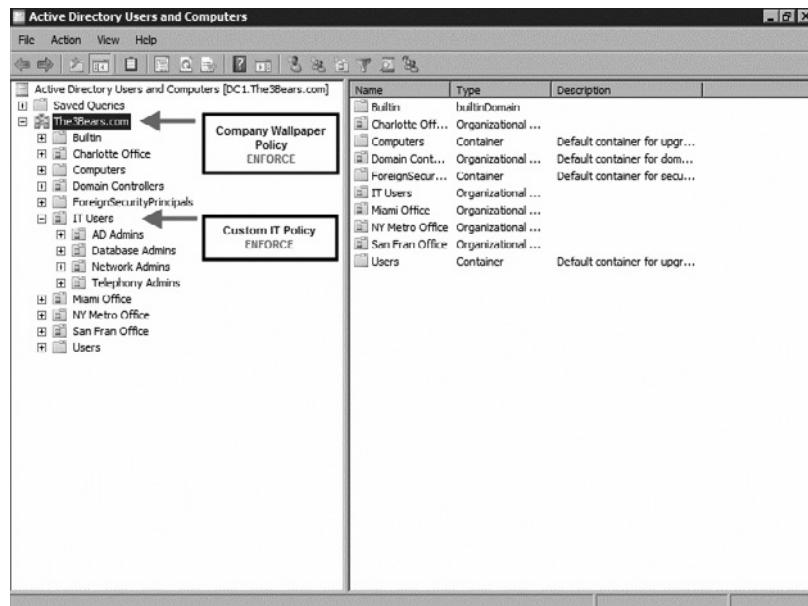
**Figure 2.28** Enforcing a GPO



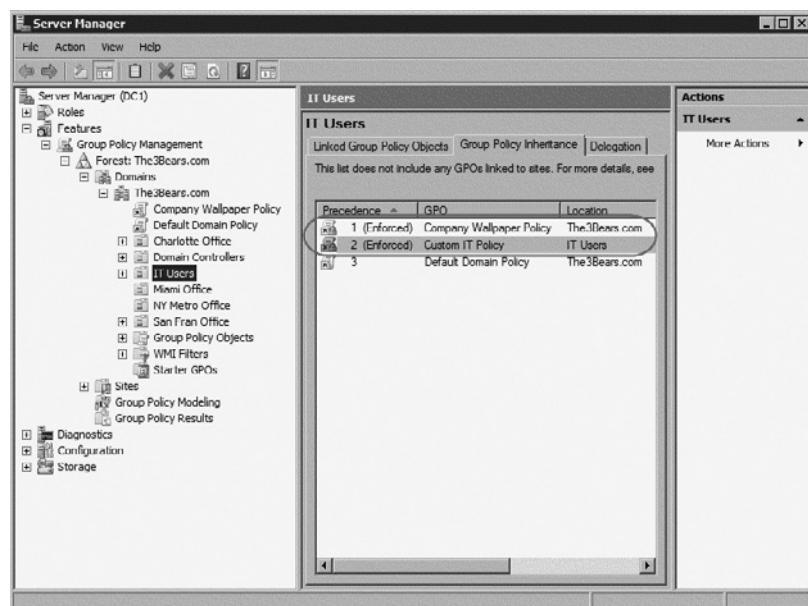
In the case of two policies set to Enforce with opposing settings, the administrators have to duel to the death and the last one standing gets to apply their policy. All right, so maybe it doesn't work quite that way. It actually goes something more like this: When two policies are both set to enforce and have conflicting values the policy *higher* in the tree structure wins (see Figure 2.29). The concept being that if you have set permissions at the domain level to apply policies the probability is that you have more clout in your Active Directory world. To reference the previous example, if both the policies to apply wallpaper were configured with Enforce, the higher "Company Wallpaper Policy" would be the resultant set winner. So there is no way for a lower level policy to attempt to override a policy higher in the tree.

structure with an Enforce. Figure 2.30 shows the Company Wallpaper Policy at the domain level which will win in the event of a conflict. Sorry IT fellas.

**Figure 2.29** Higher Level Enforce Wins



**Figure 2.30** Higher Level Enforce in GPMC



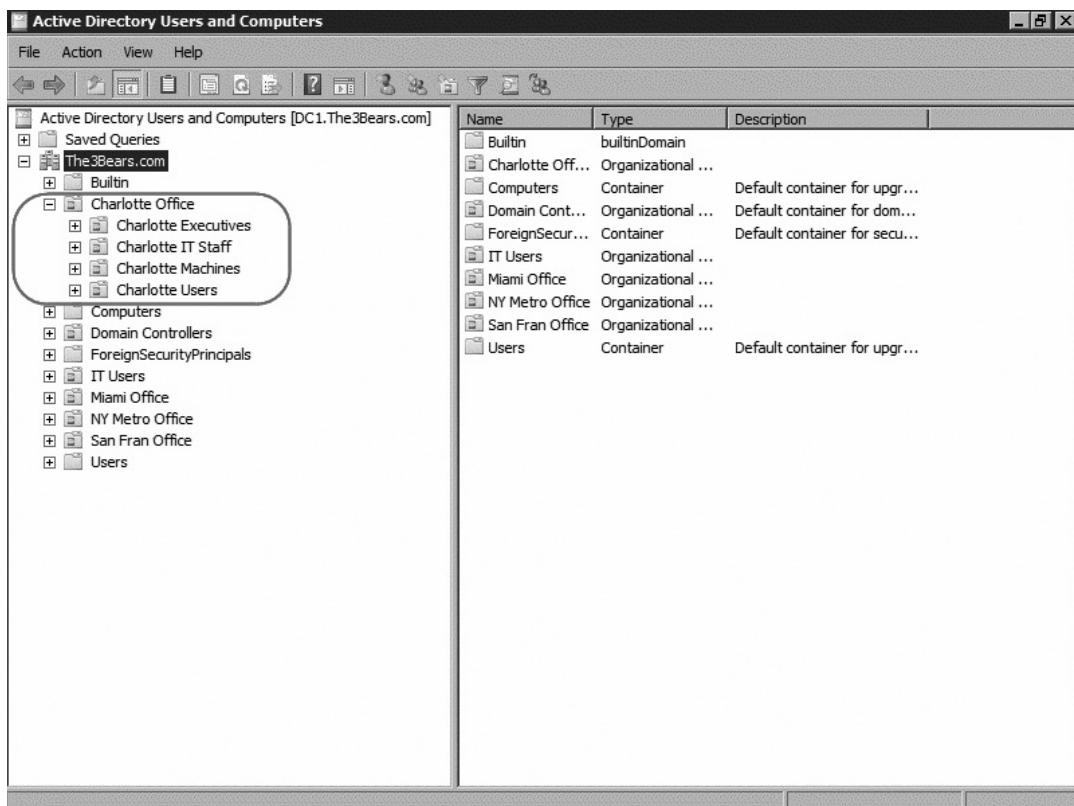


### TEST DAY TIP

Try not to panic if the exam throws a million policies at you to compare. One of the best ways to work through multiple policies is to take advantage of the paper you will have available to you during the exam. Being able to draw out the AD hierarchy and then write in the policies at your own pace can help to simplify the question. Just work through it one at a time—and don't forget—breathe!

## Block Inheritance

An additional method of manipulating default inheritance is to apply Block Inheritance to a particular OU. With this setting configured on an OU it will not inherit or apply any of the policies linked to its parent objects. The only exception to this is the Enforce setting. Enforce will barrel through a Block Inheritance and allow a policy to apply to objects within that OU regardless of the existence of Block Inheritance. If you need to isolate a lower level OU from inheriting GPOs from its parents, the easiest way to achieve this is via Block Inheritance. A wonderful utilization of this feature often involves Administrators like you. Let's assume that you would like to apply a policy that removes the Run line and the Control Panel from all users in the Charlotte office. You create and configure your policy and then link it to the Charlotte Office OU in Figure 2.31.

**Figure 2.31** Charlotte Office OU Structure

The default behavior is for the policy to trickle down the tree structure and apply to all objects in its path. This will include all objects in the child OUs. If your user account or those of your fellow administrators happen to reside in the Charlotte IT Staff OU you will inevitably be impacted by the policy. Try performing your job as an administrator without a Run line or Control Panel! The solution in this instance could be to Block Inheritance at the Charlotte IT Staff OU. By configuring a Block Inheritance the harmful policy will not be inherited by objects within the Charlotte IT Staff OU and you will retain your Run line and Control Panel. However, there can also be drawbacks to implementing this mechanism and it should only be used after careful planning. Suppose there is another policy configured at the Charlotte Office OU. This policy maps network drives to home drives for all Charlotte personnel, and runs Logon scripts. By putting a Block Inheritance in place at the Charlotte IT Staff OU the desired policy will also be blocked. As you can see, Block Inheritance can be a very powerful

disrupter in your environment, but when applied properly should become a significant addition to your administrative arsenal.

## GPO Backup and Recovery

Just as GPOs are critical to any Active Directory environment, backing them up in order to restore them in the event of a failure is critical as well. The GPMC give you the ability to Backup and Recover your GPOs. There are many reasons why backing up your GPOs on a regular basis just makes for good sense, but it also pays to give some thought to backing up your GPOs before you modify them. Just as you would perform testing on application upgrades and backup your application data before and most likely after the upgrade, similar steps should be taken when dealing with GPOs. Testing is important but being able to roll back undesirable changes is also key. Sometimes even the most thorough testing cannot root out all the potential issues you may encounter when rolling a change into production. Because of this it is a good idea to have a rollback plan in place in order to be able to execute it if required.

To backup all GPOs in a domain using GPMC follow these steps:

1. Click **Start | Server Manager**.
2. Expand **Features | Group Policy Management | Forest | Domains**.
3. Expand the domain name, for example **The3Bears.com**.
4. Select **Group Policy Objects** and **Right click**.
5. Select **Back Up All...** from the menu.

You also have the ability to backup a single GPO at a time if you prefer. In general it is a safe idea to keep up-to-date backups of your Group Policies. Restoring GPOs from backup is also accomplished via the GPMC.

## Troubleshooting

Troubleshooting GPO problems can be both frustrating and difficult without the proper tools. If you have kept good documentation of what is contained in each policy in your environment it may prove easier to determine why, for instance, Brenda from Accounting now has four extra desktop icons and a purchasing application she doesn't require after logging on Monday morning. If you haven't kept good documentation you now face the task of attempting to unravel the

tangled web of inherited policies affecting a user. Not to mention the Block Inheritance and Enforce that may also exist for you to unravel. The right tools can make your documentation insufficiency go away. By taking advantage of Microsoft built-in tools you can cut your troubleshooting time down and come to the root cause of issues with speed and grace in many situations. The two built in tools that we will review are the Group Policy Results tool and the Group Policy Modeling tool.

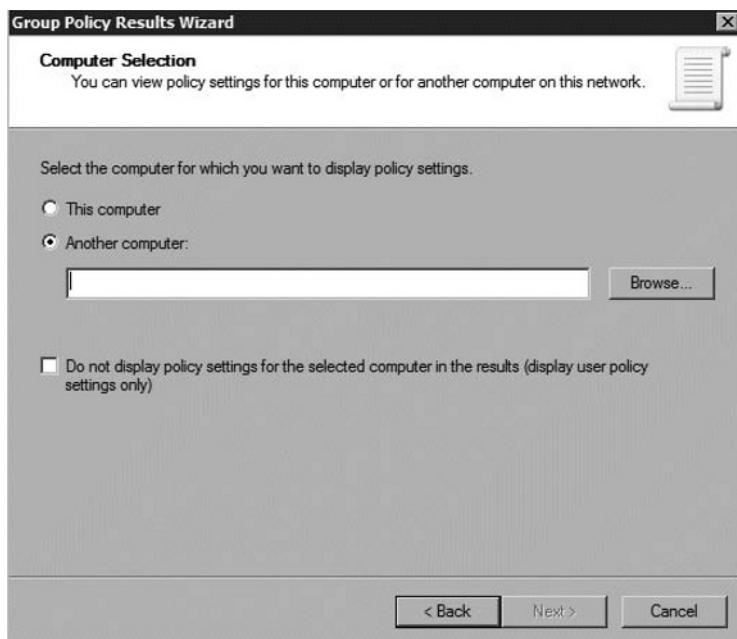
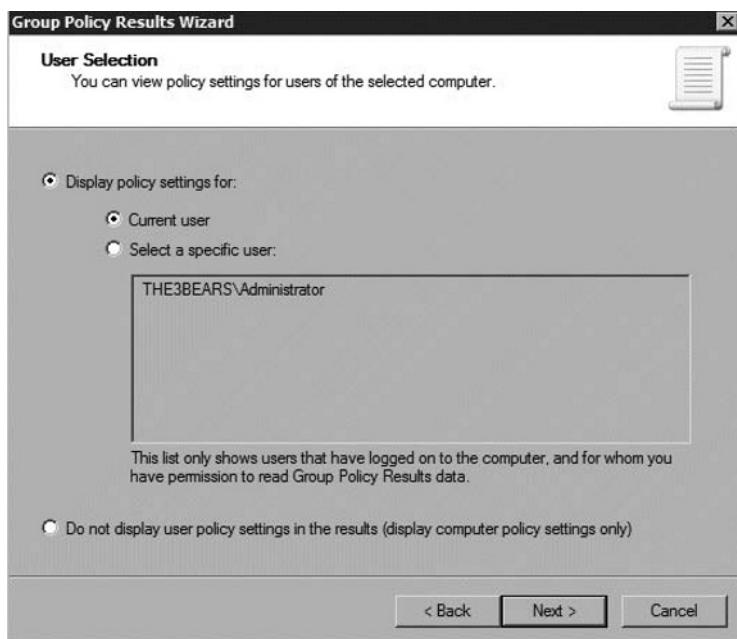
## Group Policy Results and Group Policy Modeling

When Block Inheritance and Enforce start to wreak havoc on the outcome of the policies in your hierarchy there are mechanisms you can employ to become aware of conflicts and either predict or mitigate them before real trouble brews. Microsoft provides two tools within the Group Policy Management Console which will assist you in managing and troubleshooting Group Policy in a proactive and efficient manner:

- Group Policy Results
- Group Policy Modeling

The Group Policy Results Wizard allows you to view the outcome of your policies after all have processed, applied, and the dust has settled. To execute the tool from within the GPMC simply expand the **Forest** node and select **Group Policy Results**. Right-click on **Group Policy Results** and select the **Group Policy Results Wizard**.

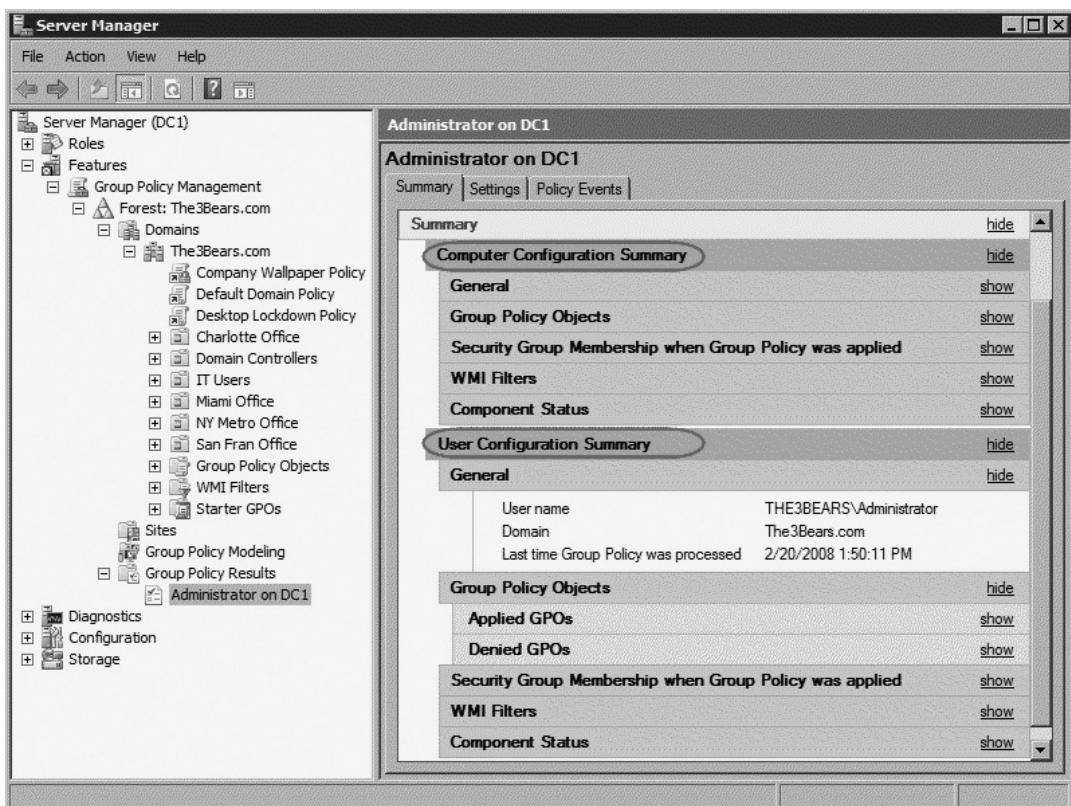
The wizard requires you to select a machine account as a first step (see Figure 2.20). It will then connect to the machine you have indicated and list all the user accounts that have logged on to the machine before. You may then select the **Current user** option or a user from the displayed list of accounts available for policy processing (see Figure 2.21). The wizard will proceed to evaluate the combination of machine account and user account policies and display the cumulative results in the details pane. You have the ability to exclude either the user or computer account from the processing if you wish. To exclude the computer policy settings use the check box labeled “**Do not display policy settings for the selected computer in the results (display user policy settings only)**” on the **Computer Selection** screen as seen in Figure 2.32 or to exclude the user policy settings use the radio button labeled “**Do not display user policy settings in the results (display computer policy settings only)**” visible on the **User Selection** screen in Figure 2.33.

**Figure 2.32** Selecting a Computer Account**Figure 2.33** Selecting a User Account

The wizard will then gather the information it requires to generate a report which will display in the Console window in the Details Pane. The report is broken down into three tabs:

- Summary
- Settings
- Policy Events

The **Summary** tab is divided into user and computer sections and displays an overview of the results (see Figure 2.34). The **Settings** tab contains the summation of each policy setting from all the contributing GPOs. The “Winning GPO” for each setting is also identified here. The **Policy Events** tab pulls from the Event Viewer of the target machines and displays any Event Viewer messages related to Group Policy. Using information from the three tabs you will be able to determine which settings are applied and where they are originating. You will also be able to determine if any errors or warnings involving Group Policy are being logged, as well as the last time Group Policy was successfully applied. Also, any queries you create will display in the console. They can be rerun, renamed, or deleted at any time. The query results can be saved out as a report in an XML or HTML file format for later review. This is a fabulous tool when trying to decipher issues involving Group Policy application in your environment!

**Figure 2.34** Displaying the Group Policy Results

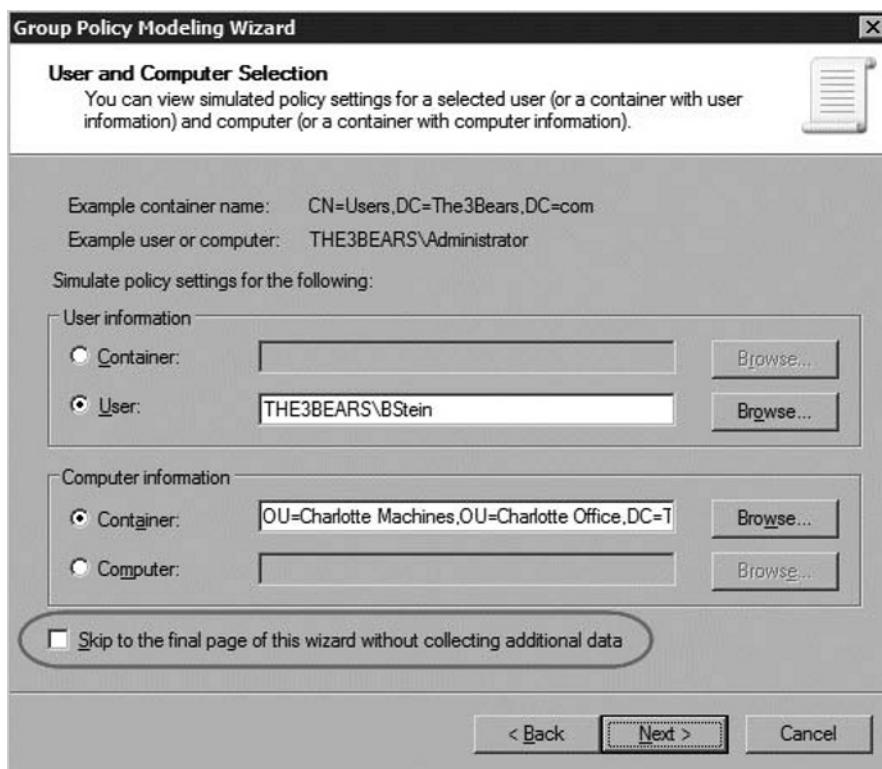
So here comes the way to attempt to *avoid* Group Policy issues in your environment, instead of resolving them as they occur. Just as Group Policy Results will evaluate the cumulative results of policies and display the results Group Policy Modeling will do the same. The difference is that with Group Policy Modeling you can explore the realm of “what if” before you actually implement the change. So “what if” Sabrina from Accounting has her user account moved into the Finance OU? Instead of relocating the user account in Active Directory and then crossing your fingers and hoping for the best you can choose to proactively employ the Group Policy Modeling tool to perform an analysis *before* the move is actually performed. The tool will tell you what Sabrina’s policy outcome will be after the move has occurred, allowing you to make an educated decision as to whether this would be smart or not.

The **Group Policy Modeling Wizard** has flexibility in that it allows you to select all the “what if” details involved in Group Policy processing to create

almost any fictional situation possible within your Active Directory environment. You launch the wizard from within the GPMC by expanding the **Forest** node and selecting **Group Policy Modeling**. Right-click on **Group Policy Modeling** and select the **Group Policy Modeling Wizard**.

The first step in the wizard is to select a domain controller able to execute the simulation. The DC you select must be running Windows 2003 or later. The next step is to identify the targets for the simulation. You can choose to specify both user information and computer information or you may only identify one of the two. Under **User Information** you can select either a specific user or a container within Active Directory. The same is true for **Computer Information**, you may select either a specific computer account or a container. Once you have selected the target for the simulation you then have two choices in what comes next: select the check box at the bottom of the window and skip to the end of the wizard (see Figure 2.35) to receive the analysis results, or click **Next** and continue to provide criteria for the simulation.

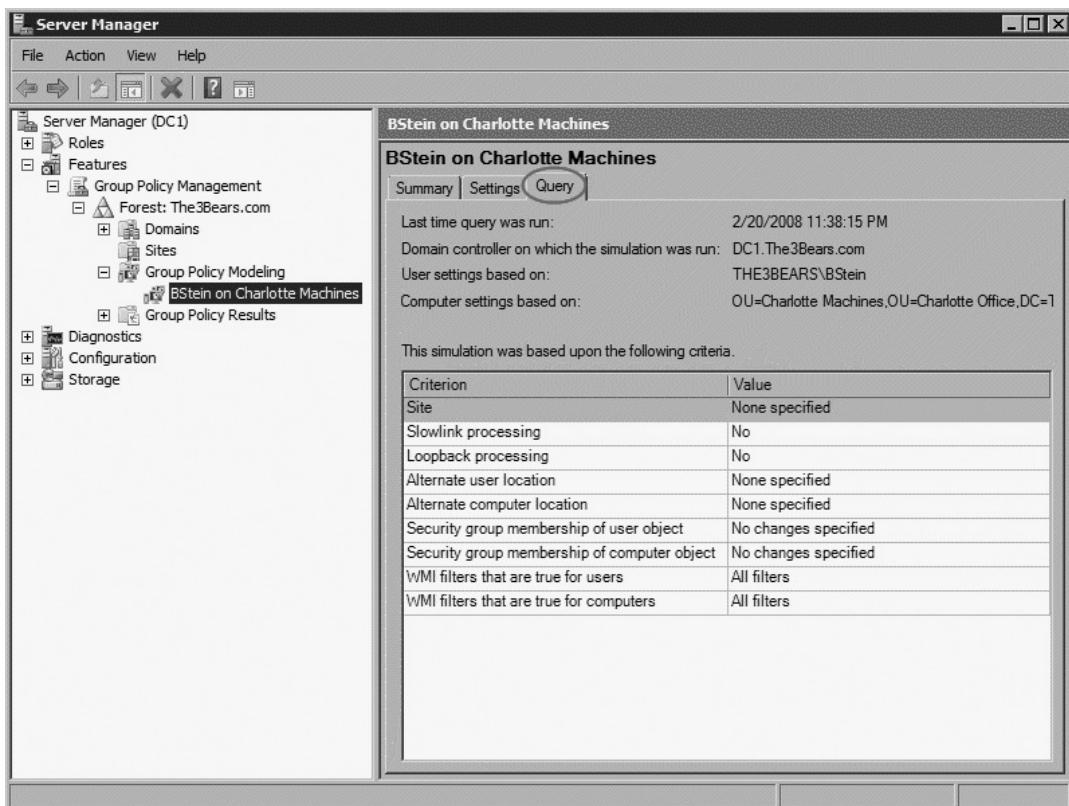
**Figure 2.35** Group Policy Modeling Wizard



If you choose to click **Next** and transverse the wizard you will be asked to lay out the scenario by providing information such as:

- Policy implementation settings
  1. Slow link processing consideration
  2. Loopback policies consideration
- Site association
- New network locations
- Security group membership
  1. For the user
  2. For the computer
- WMI Filters
  1. For the user
  2. For the computer

Once you have fed the wizard all it needs to know about your hypothetical situation it will process the policies and display the results across three tabs. The first two tabs are the same as with the **Group Policy Results** wizard: the **Summary** and **Settings** tabs. The third one differs. With Group Policy Modeling the third tab contains information on the Query that was executed (see Figure 2.36). So by reviewing the outcome of your Query you can make a determination as to whether your planned change is a wise decision or not. If the results of your simulation are not quite as you expected you can just start over again, or if you prefer you have the ability to copy existing queries. By using existing queries as a baseline you have the ability to tweak the options selected in the wizard to see what different case scenarios will yield as results until you discover a favorable outcome.

**Figure 2.36** Group Policy Modeling Query tab

## Summary of Exam Objectives

Server Management can be accomplished utilizing a variety of mechanisms and tools in Windows Server 2008. Before looking at the technology involved in server management it is recommended that administrators first take the time to develop a management strategy. Once a strategy has been developed for an organization, administrators should look to the tools to be used to execute the strategy. Remote Administration in Windows Server 2008 is made possible with Remote Desktop as well as through the installation of RSAT on administrative workstations. While Remote Desktop allows access directly to any server in the organization RSAT allows administrators to utilize their own workstations by connecting to services remotely through MMC snap-ins. Instead of logging onto servers directly administrators have the flexibility of using the tools included with RSAT to connect to multiple servers spread across the organization.

Windows Server 2008 also includes many management technologies and features. Some of the available server management tools include:

- Server Manager
- Windows Powershell
- Windows Deployment Services
- Windows Reliability and Performance Monitor

Server Manager allows the administrator the ability to deploy new server roles and manage features of Windows Server 2008. Windows Powershell is a command line interface which allows for the creation of powerful scripting to perform daily maintenance tasks, and Windows Deployment Services have replaced the Windows Server 2003 RIS services.

Group Policy is a powerful tool that you can use to lock down and configure many different aspects of your environment. Two major kinds exist:

- Local Group Policies
- Non-local Group Policies

Local Group policies contain settings that apply to user accounts on the local machine as well as local computer settings. With Windows Vista and Windows Server 2008, Multiple Local Group policies can be configured. Multiple Local Group policies allow you granularity by giving you additional policies based on user type.

Non-local Group Policies exist in an Active Directory domain and are stored on Domain Controllers. Settings within GPOs come in two flavors: User Configuration

and Computer Configuration. Within each of those flavors at the domain level there are Policies and Preferences. Policies are enforced and Preferences are only set. Users can adjust preference settings after they are configured on their machines. They cannot adjust policy settings. GPOs can be created, created and separately linked, or created and linked in one action. GPOs can be applied at the Site, Domain, or OU levels. All policies inherit *down* the tree structure from where they are applied. You can control that behavior by using GPO features like Block Inheritance, Enforce, and Filtering. Block inheritance will prevent *all* policies from parent OUs from inheriting. The only exception to that is a policy configured with Enforce. Enforce is configured per policy and it will barrel through Block Inheritance. Enforce always wins in the event of a conflict regardless of where the Enforce originates from—above or below the conflicting policy. If two policies configured with Enforce conflict, the one higher in the tree structure wins.

Policies are extensible and additional configuration settings are made available through ADM and ADMX files. The ADM files are the traditional administrative file and contain additional settings, usually application specific. They use a custom markup language and are stored with the policies' GPT of a GPO within SYSVOL. The ADMX files use an XML format and are stored in a Central Store within SYSVOL. Security Templates and StarterGPOs assist in duplicating administrative effort across the enterprise. Security Templates are stored in an INF file format and can be imported into GPOs for uniform application of security settings. StarterGPOs allow the creation of baseline GPOs. They can be exported to a CAB file format and ported to different domains and forests easily.

## Exam Objectives Fast Track

### Developing a Management Strategy

- Remote Desktop gives you the flexibility and security you need as an administrator to be more productive in your day-to-day tasks.
- Server manager is the primary tool for add/remove of roles and features for Windows Server 2008.
- Use the performance tools to track the health of your servers over time.

### Delegating Administration

- Delegate at the OU or Domain level when possible.
- Keep your delegation simple and document well.

- Stay away from delegation that is too broad in nature. Try to use the principle of least privilege for your delegations.

## Planning a Group Policy Strategy

- Use the proper GPO setting type: Policies for enforced settings, Preferences for user configurable settings.
- Remember to consider carefully and document well if you decide to implement Enforce and Block Inheritance.
- Understanding inheritance is critical to planning a group policy strategy.

## Creating and Linking Group Policy Objects

- In order to utilize Group Policy Objects (GPOs) you must first become acquainted with how to create them in your Active Directory environment.
- Once you have created a Stand-alone GPO it will affect no person or machine in your environment. In order to have your new policy have an impact on your network you must link it somewhere in the hierarchy.
- Just as GPOs are critical to any Active Directory environment, backing them up in order to restore them in the event of a failure is critical as well.

## Controlling Application of Group Policies

- The nature of Group Policy inheritance and the hierarchy of Active Directory can sometimes create unfavorable conditions, causing a policy to fail to apply where it is required.
- To prevent a mandated policy from being overridden you must mark the link as Enforced.
- An additional method of manipulating default inheritance is to apply Block Inheritance to a particular OU.

# Exam Objectives

## Frequently Asked Questions

**Q:** What is Remote Desktop and why will I use it?

**A:** Remote Desktop is a tool which gives you the ability to log on to any server in your environment from anywhere else in the environment—remotely. Most administrators find it very useful in performing their day-to-day duties without needing to install local tools or actually go to the servers physically.

**Q:** What tools are available for Remote Administration in Windows Server 2008?

**A:** Remote Desktop, Remote Server Administration Tools, and Windows Powershell scripting.

**Q:** What is Group Policy and why is it used?

**A:** A Group Policy is a collection of settings and configurations that can apply to either a computer or a user and work together to establish a user's working environment. The administrator can utilize Group Policy to enforce restrictions, provide software, or even configure security settings in their environment.

**Q:** Why is Delegation useful in my environment?

**A:** Instead of granting all administrators full-control permissions, delegation allows you to create an environment which recognizes differences in administrative scope. You can match the permissions you grant an administrator with the job function they perform. This creates a safer and more secure environment with less chance for accidental problems related to administrative function.

**Q:** What is Server Manager?

**A:** Server Manager is the new utility for role- and feature-based administration on Windows Server 2008. It allows you to add, remove, and configure the available roles and features on a given Windows Server 2008 machine.

**Q:** What exactly is a Computer Loopback policy?

**A:** A policy that allows you to control where user settings come from that apply to a particular machine. The user settings applied to the machine are pulled from the computer policy affecting the machine. The user settings from within the computer policy are either Merged with the user's settings, or they replace them.

In environments where public machines exist this policy will come in very handy. Companies that commonly have kiosks and public access computers, like lab environments or libraries, will find these policies handy.

**Q:** What is a StarterGPO and what is it for?

**A:** A StarterGPO is a policy that allows the administrator to create a baseline which contains frequently used settings. This policy creates reuseability because it can be used as a starting point when creating additional GPOs in the organization, therefore reducing administrative effort.

**Q:** What is RemoteApp?

**A:** RemoteApp is a new feature in Terminal Services for Windows Server 2008 that allows you make applications available to users through an icon rather than having to log on to the server desktop to launch applications.

**Q:** What is new with Group Policy in Windows 2008?

**A:** Windows 2008 has the following new features to offer in Group Policy:

- Comments for GPOs and policy settings
- New ADMX file format for Administrative Template settings
- Starter GPO capabilities
- Preferences
- Network Location Awareness
- Multiple Local Group Policies

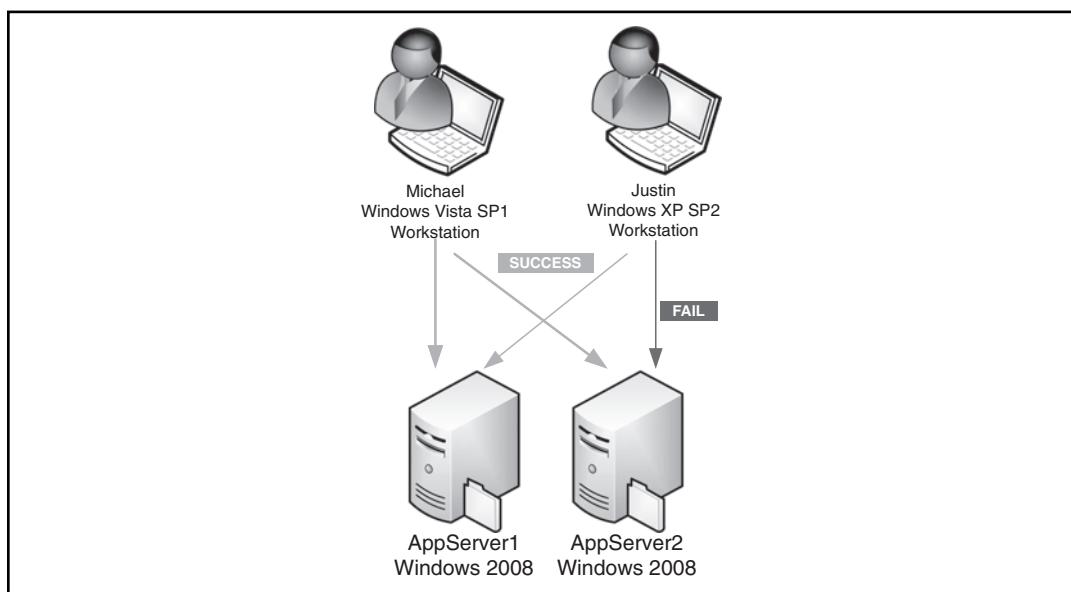
**Q:** What is TS Web Access (TWSA) and why will I use it?

**A:** TWSA allows administrators to create a Web page where Terminal Services applications are made available via icons which will launch the application remotely. The benefit in using TWSA is that it gives you the ability to have a central location in which to update RemoteApp applications. Changes to the way an application is accessed would require only a single change on the TWSA server and would not require the change to be pushed to machines in the organization.

## Self Test

- Justin and Michael are administrators for a large financial firm. They are in the midst of a server deployment project and have decided to configure Remote Desktop for the eight new application servers they will be installing. All of the new servers will run Windows 2008 and will have a custom financial application installed. Once the first pair of servers has been installed with Windows 2008 and configured for Remote Desktop Justin and Michael decide to test their connectivity so that they can finish their application installs remotely. Michael is able to log on to both new servers, AppServer1 and AppServer2. Justin is able to successfully log on to AppServer1, however he is not able to successfully log on to AppServer2. Justin and Michael are both members of the Remote Desktop Users group (see Figure 2.37).

**Figure 2.37** Justin and Michael's Log-on Attempts



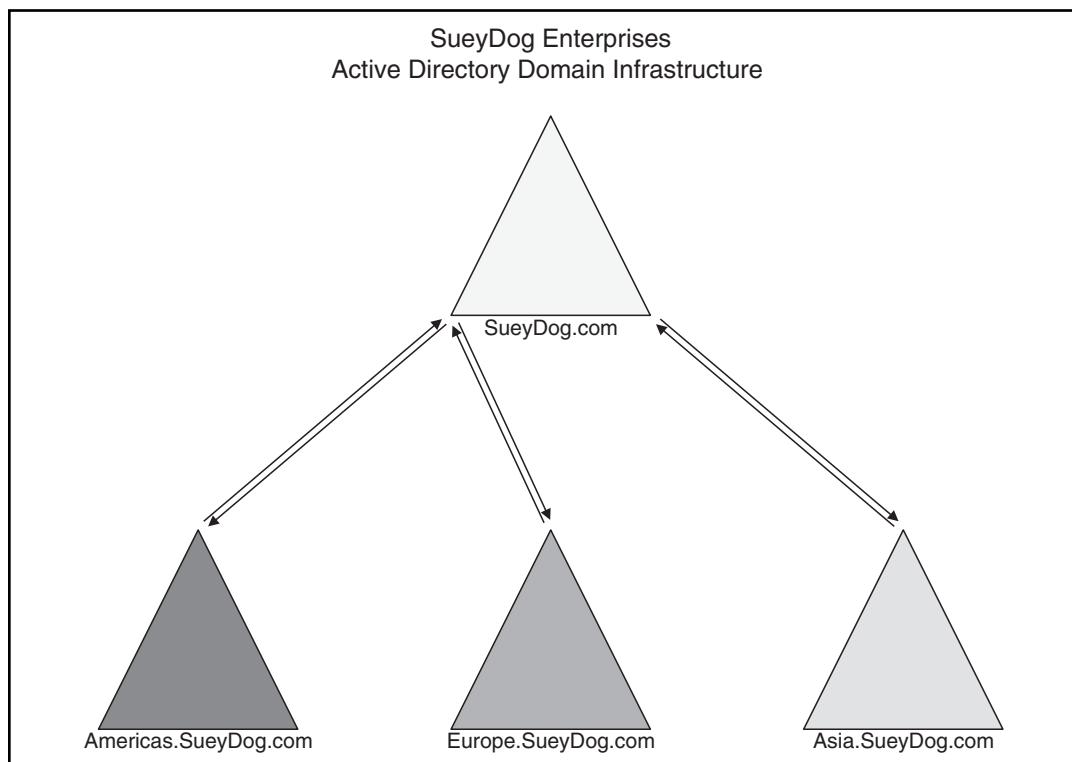
Which of the following will allow Justin to authenticate against AppServer2 with the least amount of effort?

- Both Justin and Michael must be members of the Domain Administrators group.

- B. AppServer2 should have the Remote Desktop configuration adjusted to “**Allow connections from computers running any version of Remote Desktop (less secure)**”.
  - C. Justin must upgrade his workstation to Windows Vista.
  - D. Justin and Michael must install the MSTSC 6.0 on their workstations.
2. Your company is growing at a rapid pace and you find yourself presented with new lock-down settings from management every few weeks that need to be propagated out to different user departments. You have been creating a new GPO for each setting and then linking the new policies to the domain level or departmental OUs. Some users are starting to complain that it is taking a long time to log on and view their desktop. What is most likely the root cause in the logon slow down?
- A. Your Active Directory domain controllers are too slow and need to be upgraded.
  - B. Users are downloading an increasing number of policies; therefore logon is slowed because the user workstations need to be upgraded since the HW is old and substandard.
  - C. Users are downloading an increasing number of policies; therefore logon is slowed while the machines wait for policies to process and the settings to apply.
  - D. Users are downloading an increasing number of policies; therefore logon is slowed due to insufficient bandwidth.
3. You need to create and apply a new Security Template for all of the database servers in your environment. Place the following steps in the correct order to accomplish this.
1. Open a Custom MMC
  2. Add the Security Templates Snap-in
  3. Open Server Manager
  4. Edit your GPO
  5. Drill down to the Security Settings section of the GPO
  6. Right click the Security Settings section of the GPO and select to Import Policy
  7. Configure your new Security Settings

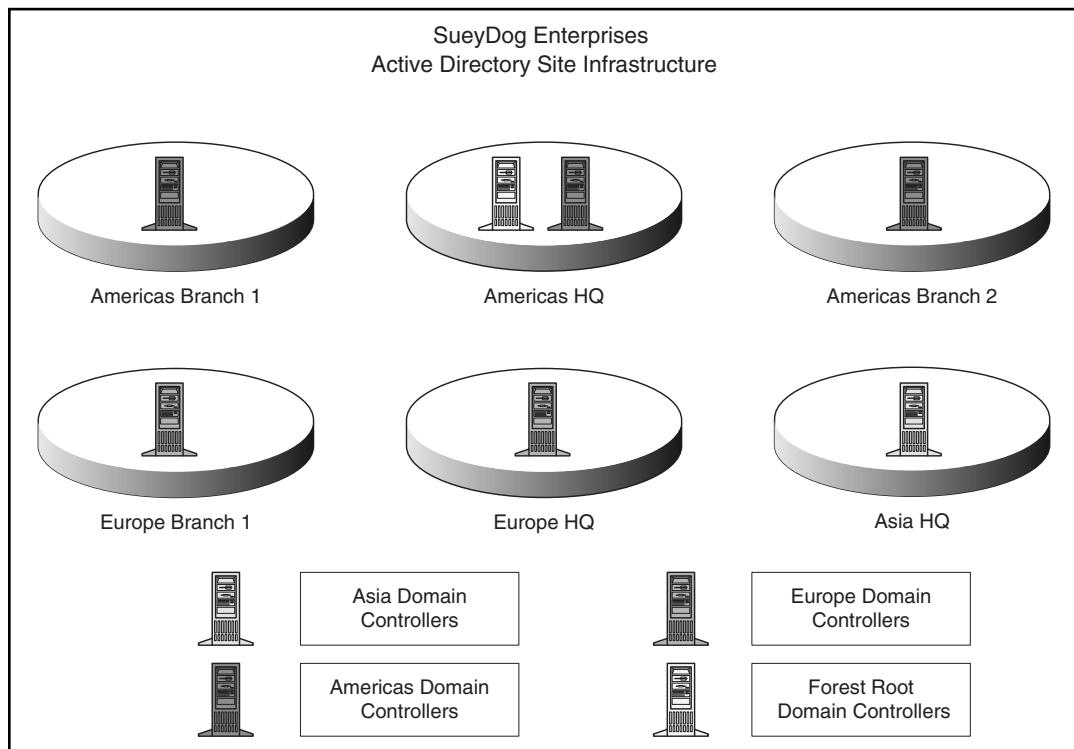
8. Connect to the preferred storage location for Security Templates in your environment
9. Create a new Security Template
10. Save the Security Template
11. Select the correct .inf file from the list of available files
12. Browse to the location of the .inf files in your organization
  - A. 1,4,5,7,9,2,3,6,8,10,12,11
  - B. 1,2,8,9,7,10,3,4,5,6,11,12
  - C. 3,4,7,9,10,1,2,5,8,12,6,11
  - D. 3,4,9,5,6,10,8,11,2,7,1,12
4. You are creating a new Group Policy that needs to be applied across two domains in your environment. The policy has approximately 350 settings. Your domain structure is depicted in Figure 2.38:

**Figure 2.38** SueyDog Enterprises AD Structure



You decided that to save time and administrative effort you will create the policy at the site level. The users that require the policy exist in America and Europe only. You link the policy to all of the Americas and Europe sites. Your Site structure is depicted in Figure 2.39.

**Figure 2.39** SueyDog Enterprises Site Infrastructure

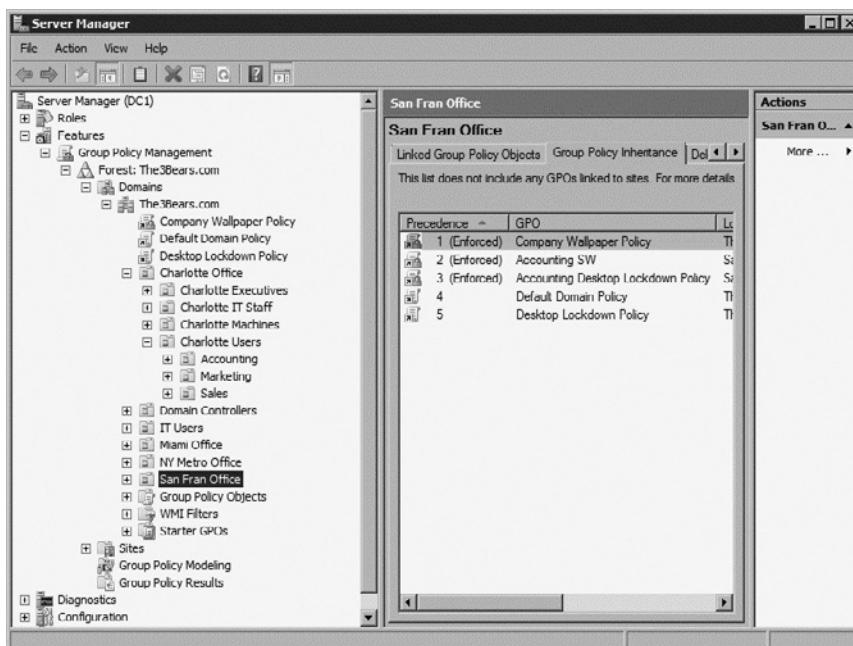


The next day users begin complaining that log-on time has increased dramatically in Europe. Only some of the Americas users are complaining about slow log-on times. What is causing this problem?

- A. The domain controllers cannot handle such a large policy.
- B. The policy is too large and the client machines cannot handle such a large policy.
- C. Creating the policies at the Site level.
- D. The policy hasn't replicated to Europe or the branch offices in the Americas yet.

5. Darien is a new member of the Web Services team at your company. He is going to be responsible for running and testing scripts for an in-house home-grown application which requires a special application that is deployed via Group Policy. The first time he logs onto the domain he does not receive the software package. You verify that his user account is in the proper OU. What could be causing Darien not to receive the GPO with the software policy?
- Security filtering has been enabled on the GPO and Darien is not a member of the proper group.
  - WMI filtering has been enabled on the GPO and Darien is not a member of the proper group.
  - Darien must be a local administrator on his machine in order to download a GPO with a software package in it.
  - Darien's user account has Block Inheritance configured on it and therefore he cannot download the policy.
6. Here is an image of your Active Directory Organizational Unit Architecture (see Figure 2.40).

**Figure 2.40** Active Directory Image



As the administrator of The 3Bears Inc. you need all computers in the Charlotte office to be configured with a new Power Scheme. You create a Group Policy with the desired configuration and you need to select an OU to apply the settings. Which OU would you select to apply the policy?

- A. Charlotte Office
  - B. Charlotte Executives
  - C. Charlotte Machines
  - D. Domain Level
7. SueyDog Enterprises will soon be deploying Microsoft Office Communicator into their environment. All of their domain controllers are running Windows Server 2008. Their administrator Matthew is attempting to prepare for the new product by creating a GPO and exploring the available settings. He creates a new policy and proceeds to expand each section of the policy looking for the section containing the Microsoft Office Communicator settings. He can't seem to locate the settings for Microsoft Office Communicator. What should Matthew do to gain the settings he seeks?
- A. Download the appropriate ADM file and import it into the new GPO.
  - B. Install Microsoft Office Communicator on the domain controller to make the setting available.
  - C. Download the appropriate ADMX file and import it into the new GPO.
  - D. Download the appropriate ADM file and place it in the Central Store.
8. Joey is going to be migrating his Lotus Notes environment into his newly established Windows Server 2008 forest. He has guidance on what he will require for Group Policy settings for the different teams and departments. He has not yet created his OU structure. How should Joey proceed in creating the required GPOs?
- A. Create Stand-alone GPOs.
  - B. Create the GPOs at the Domain level.
  - C. Create the GPOs at the Site level.
  - D. Wait to create the GPOs until the OU structure is in place.

9. How would you troubleshoot the following error message (Figure 2.41):

**Figure 2.41** Remote Desktop Connection Error Message



- A. In the Remote Desktop Connection client select **Options | Advanced** and adjusted your authentication choices.
  - B. On the **System Properties | Remote** tab select "**Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**"
  - C. On the **System Properties | Remote** tab select "**Allow connections from computers running any version of Remote Desktop (less secure)**"
  - D. Both A and C
10. You would like your users to be able to run a custom home-grown application in a centralized fashion. You install the application on your server and then add terminal services. You have a user attempt to connect using Remote Desktop and launch the application. The application does not work properly. How do you attempt to correct the problem?
- A. Uninstall the application, reinstall the application
  - B. Install the TS Gateway role on the server
  - C. Uninstall Terminal Services, uninstall the application, reinstall Terminal Services, reinstall the application
  - D. Uninstall Terminal Services, reinstall the application, reinstall Terminal Services

## Self Test Quick Answer Key

- |             |              |
|-------------|--------------|
| 1. <b>B</b> | 6. <b>C</b>  |
| 2. <b>C</b> | 7. <b>A</b>  |
| 3. <b>B</b> | 8. <b>A</b>  |
| 4. <b>C</b> | 9. <b>C</b>  |
| 5. <b>A</b> | 10. <b>A</b> |

# Chapter 3

## MCITP Exam 646

### Monitoring and Maintaining Servers

#### Exam objectives in this chapter:

- Patch management
- Monitoring for Performance

#### Exam objectives review:

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

# Introduction

One of the most important, and overlooked, tasks as an administrator involves monitoring and optimizing our servers. This has become somewhat of a science with many third-party independent software vendors providing solutions. Microsoft has many of the tools within Microsoft Windows 2008 Server needed to optimize and monitor servers.

The most important step of monitoring and optimizing servers involves trending and baseline analysis. A baseline analysis provides saved monitoring data to be compared to current data. This is really useful when you have performance issues and need to determine the cause or causes. This data needs to be collected during a time when users are on the system and the load is realistic—you don't want to record trending and monitoring data right after a server build with no users on the system.

Another important area this chapter is going to cover is patch management. Patch management is important to protect Microsoft Windows Server 2008 against security issues and keep the server running with the latest available software from Microsoft and independent software vendors. Like monitoring software—there are many third-party software providers that offer patch management solutions.

For the Microsoft exam, it is important to understand how to monitor and optimize Windows 2008 Server. It will also be important to understand how to install and configure Windows Server Update Services (WSUS).

## TEST DAY TIP



Information in this chapter will include items that need to be memorized for the exams. Questions concerning optimizing and monitoring are usually scenario based—it will be important to know what counters to use and how to interpret the data. I would suggest using a notebook and keep track of this data as you work through this chapter. On test day, this will make a great review tool to glance over before heading into the testing center.

## Patch Management

Microsoft has a couple of options for patch management—for both the OS Level and Application Patching. The software that Microsoft makes available free of charge is called Windows Server Update Services (WSUS). WSUS enables administrators

to deploy the latest Microsoft product updates to computers running a Microsoft Windows operating system. WSUS allows administrators to fully manage the distribution of updates that are released on their network via Microsoft Update. This application will be the only patch management application you will be tested on with this exam. Though it is freely available, WSUS is very powerful and granular in its design and implementation. The infrastructure design can be complex and has many possibilities for scenario and multiple choice-based questions.

### **EXAM WARNING**

 It is highly recommended that while studying this book, you should also do all of the exercises via hands-on labs. You can download a copy of Windows 2008 Server, WSUS and Microsoft Virtual PC 2007 for free from the Microsoft website. Go out and download these three items and design your own virtual network on your desktop PC. During the exam you will be asked to do hands-on scenario based questions. The best way to prepare for these types of questions is to do as much hands-on training as possible.

Microsoft does make a commercial product available for customers that need more than a patch management system. The product is called Microsoft Systems Center Essentials 2007. Microsoft Systems Center Essentials 2007 can manage up to 30 servers and 500 clients. If your network exceeds this limit you can purchase System Center Configuration Manager 2007—another product that Microsoft makes available. Some of the features included with Microsoft Systems Center Essentials 2007 include:

- Proactive monitoring and troubleshooting diagnostics for your Windows-based servers, Windows-based clients, applications, and network devices
- Update management for Microsoft and third-party applications and devices
- Software deployment of MSI and EXE installed software packages, including third-party applications and Microsoft Office 2007
- Hardware and software inventory with thirty-plus attributes collected for things like available disk space, RAM, and installed applications with version number
- Integrated reporting including fifty-plus reports for things like inventory update deployment status and automated daily health status reports for your IT environment

On this exam, you will not need to know anything about Microsoft Systems Center Essentials 2007 or Microsoft System Center Configuration Manager 2007. It is important though, as a network administrator, to know what options are available to you.

## OS Level Patch Management

Microsoft makes OS Level Patch Management available two different ways. The first way is via WSUS—we will go into greater detail on this in the next section. The other option is through Windows Update built into all currently supported operating systems. Microsoft makes normal updates available the second Tuesday of each month; some term this “Super Tuesday.”

Microsoft Windows 2008 Server by default has Windows Update turned off. This needs to be scheduled for automatic updates or scheduled updates. Most administrators choose to have scheduled updates; this way it does not interfere with the workday if the server needs to reboot.

### EXERCISE 3.1

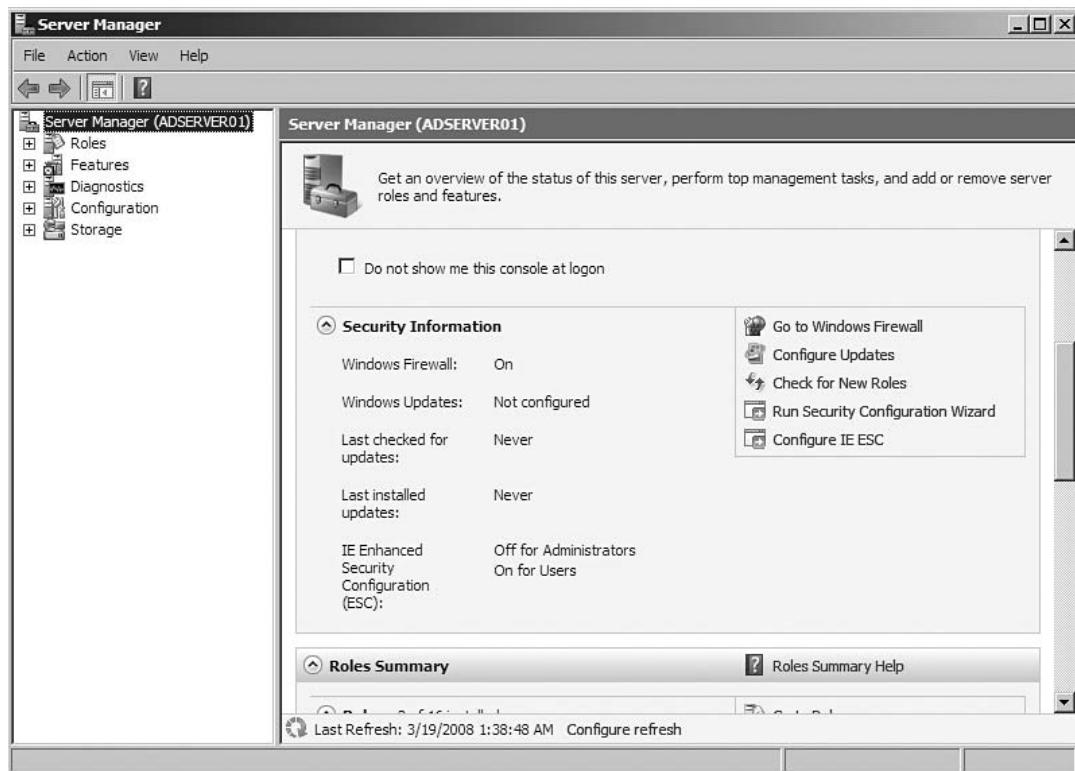
---

#### ENABLING WINDOWS UPDATE ON MICROSOFT WINDOWS 2008 SERVER

In this exercise, we are going to take ADSERVER01 and enable the Windows Update for scheduled updates. ADSERVER01 is a newly installed Microsoft Windows Server 2008 Active Directory controller for the contoso.com domain (keeping with the Microsoft lab tradition). Since this is a new server installation, Windows Update will not be enabled by default.

1. First, we will need to open the Server Manager. To do this, click on **Start | Server Manager** at the top of the Start Menu.
2. On the Server Manager, click **Server Manager** at the top of the Server Manager tree on the left side. See Figure 3.1 for help.

**Figure 3.1 Server Manager**



3. Next, click on **Configure Updates** on the right side of the Server Manager window.
4. In the **Windows Update** pop up, click **Let me choose**. See Figure 3.2 for the Windows Update pop up window.

**Figure 3.2 Windows Update**



5. In the **Choose how windows can install updates** window, select **Download updates but let me choose whether to install them** and **Include recommended updates when downloading, installing or notifying me about updates**. By selecting these two radio buttons, you will ensure that an administrator will have to intervene when an update is installed. This is particularly important when the administrator wants to test each update before installing them.
  6. Click **Ok** at the bottom of the window.
  7. Close the Server Manager by clicking **File** then **Exit**.
- 

## Windows Server Update Service

As previously discussed, Microsoft Windows Server Update Service (WSUS) is the freely available software that allows IT administrators to manage Microsoft updates in a network infrastructure. The most current version that is supported in Microsoft Windows 2008 Server is WSUS 3.0 Service Pack 1. WSUS is compatible with both Microsoft Windows 2003 Server Service Pack 1 and Microsoft Windows 2008 Server. This chapter will deal with Microsoft Windows 2008 Server only.

WSUS depends mostly on the Internet Information Services (IIS) 7.0 in Microsoft Windows Server 2008. There needs to be certain components of IIS 7.0 installed before WSUS can be installed. The IIS 7.0 components needed are:

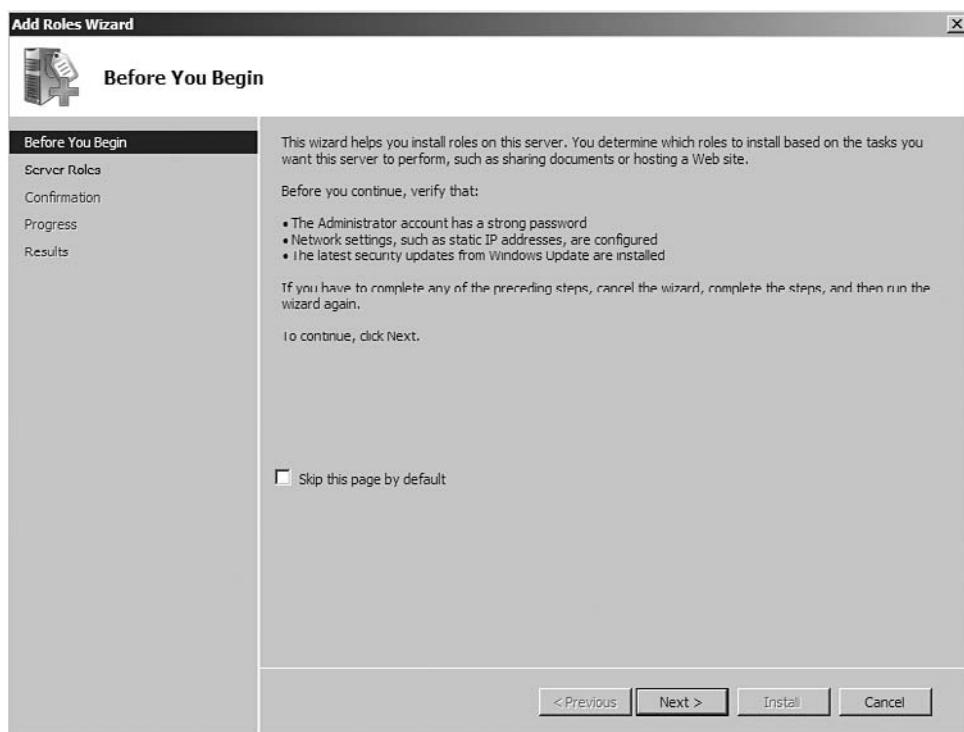
- Windows Authentication
- ASP.NET
- IIS Version 6 Management Compatibility
- IIS Version 6 Metabase Compatibility

### EXERCISE 3.2

#### INSTALLING IIS 7.0 COMPONENTS FOR WSUS 3.0 SP1

In this exercise, we are going to install the necessary IIS 7.0 components that are needed to support a WSUS 3.0 SP1 installation.

1. Click **Start | Server Manager**.
2. In the task tree on the left side of the Server Manager, right click **Roles** and select **Add Roles**. The **Add Roles Wizard** appears. See Figure 3.3 for the **Add Roles Wizard**.

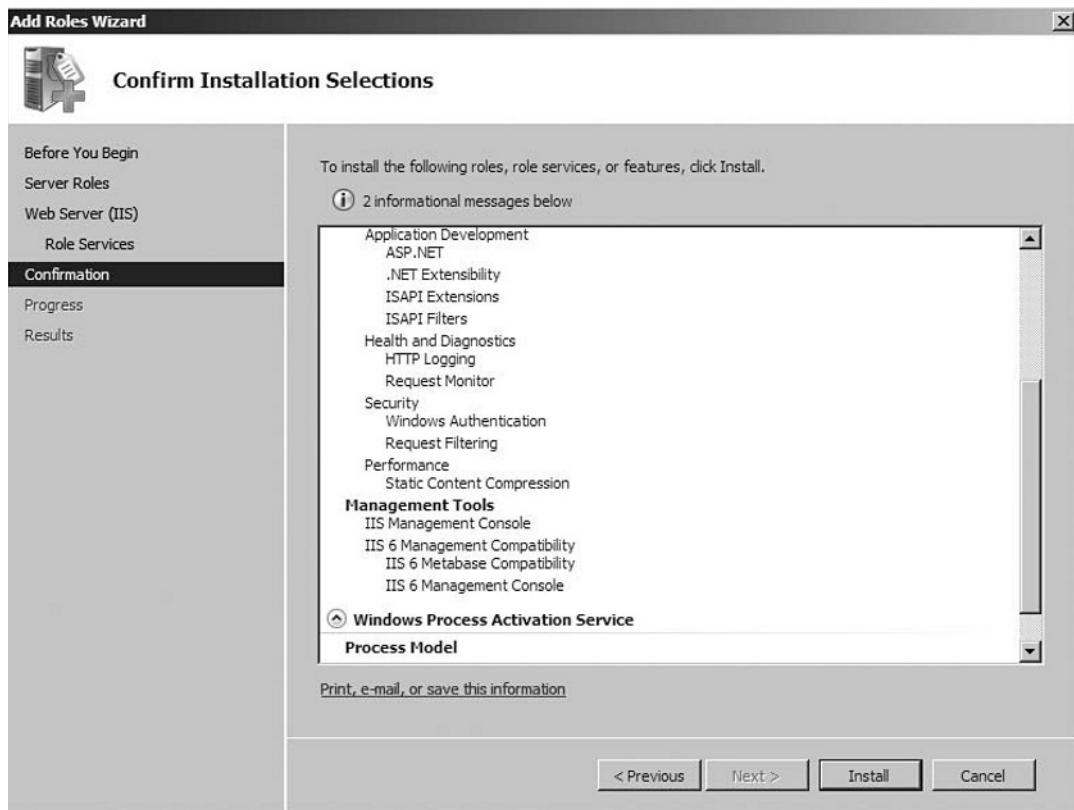
**Figure 3.3** Add Roles Wizard

3. Click **Next** to continue.
4. Check the box next to **Web Services (IIS)**. In the **Add features required for Web Server (IIS)** dialog box click **Add required features**. See Figure 3.4 for the **Add required features** dialog box.

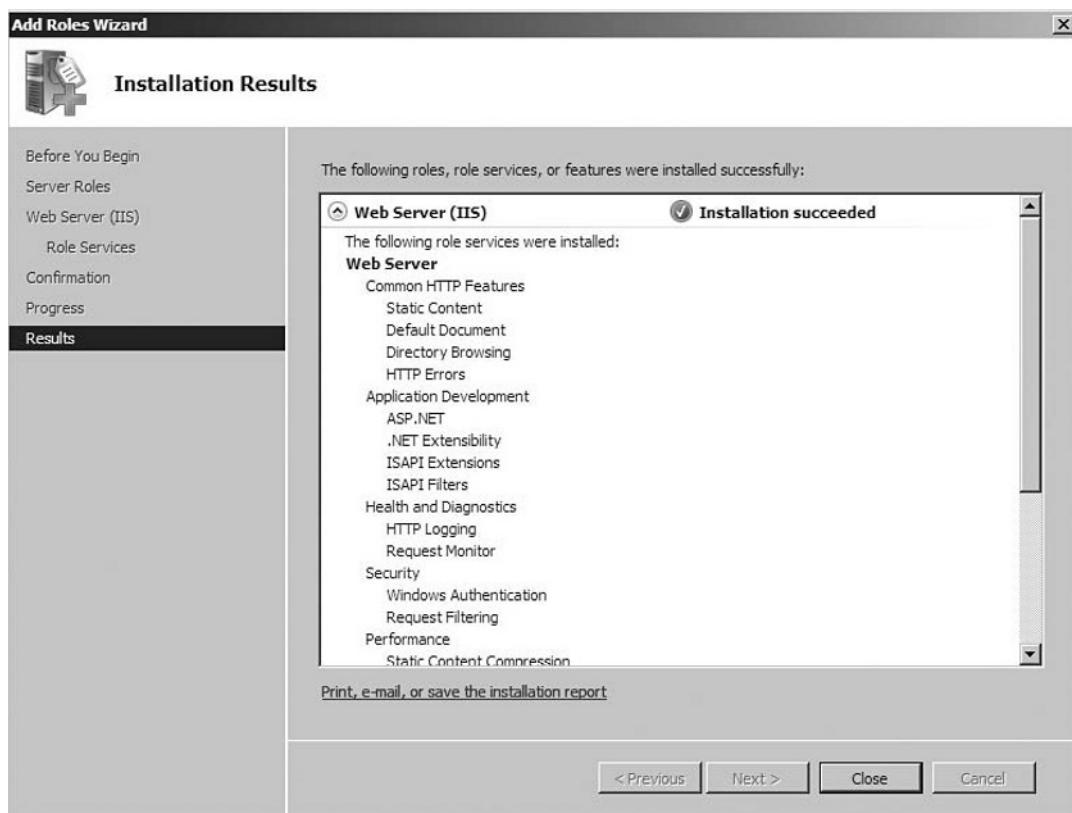
**Figure 3.4** Add Required Features Dialog Box

5. Click **Next** twice.
6. In the **Select Roles Service**, click the boxes next to **Windows Authentication**, **ASP.NET** (when prompted click the **Add required roles box** at the **Add role services and features required for ASP.NET dialog box**), **IIS 6 Metabase Compatibility**, and **IIS 6 Management Compatibility**. Click **Next**.
7. Verify the selections in the **Confirm Installation Selections** screen—see Figure 3.5. Once you are sure all selections are in the confirmation window, click **Install**.

**Figure 3.5** Confirm Installation Selections



8. After the installation, make sure the installation succeeded in the **Installation Results** screen—see Figure 3.6. Click **Close**.

**Figure 3.6 Installation Results**

- 
9. Click **File** and then **Exit** to close the **Server Manager**.

## WSUS 3.0 SP1 Deployment on Microsoft Windows 2008 Server

When you are deploying WSUS 3.0 SP1 in Microsoft Windows Server 2008, there are some software requirements that must be met before the installation can take place. As discussed earlier, IIS 7.0 is a requirement—so the software requirement list would look like this:

- Microsoft Internet Information Services (IIS) 7.0 with the following components:
  - Windows Authentication
  - ASP.NET

- IIS Version 6 Management Compatibility
- IIS Version 6 Metabase Compatibility
- Microsoft Report Viewer Redistributable 2005 (<http://go.microsoft.com/fwlink/?LinkID=70410>)
- Microsoft SQL Server 2005 Service Pack 1 (<http://go.microsoft.com/fwlink/?LinkID=66143>)

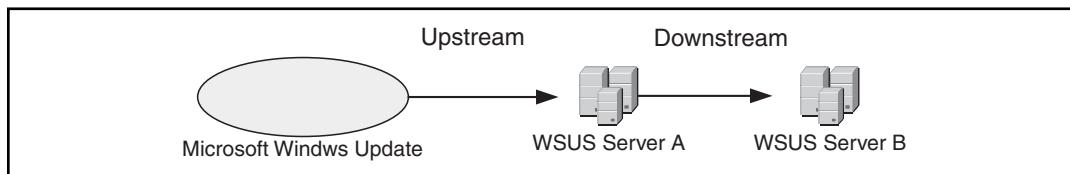
WSUS 3.0 SP1 stores update information and the updates on the server (if you choose this type of deployment). Storage is very important to a WSUS 3.0 SP1 installation—you need to plan storage requirement very carefully to prevent storage issues in the future that would require partition resizing or operating system rebuilds. The following storage requirements should be followed very carefully:

- Both the system partition and the partition on which you install WSUS 3.0 SP1 must be formatted with the NTFS file system.
- A minimum of 1 GB of free space is recommended for the system partition.
- A minimum of 20 GB of free space is recommended for the volume where WSUS 3.0 SP1 stores content; 30 GB of free space is recommended.
- A minimum of 2GB of free space is recommended on the volume where WSUS 3.0 SP1 Setup installs Windows Internal Database.

#### EXAM WARNING

It is very important to remember that WSUS 3.1 SP1 cannot be installed on a compressed drive. Check to make sure that no drives on the system are compressed. Also keep in mind the storage requirements for the system drive and where WSUS is installed.

WSUS 3.0 SP1 allows for granularity of control. When designing the server infrastructure, you can choose to have one WSUS 3.0 SP1 server as the main download server—the other WSUS servers can acquire updates from the main server. In this type of design, Internet bandwidth is conserved. This is referred to server hierarchy (see Figure 3.7). The server that downloads the updates from Microsoft is referred to as the upstream server. The server acquiring updates from the upstream server is called the downstream server.

**Figure 3.7 WSUS Server Hierarchy**

There are two modes downstream and upstream servers can be when connecting them through a WSUS server hierarchy. The modes determine how the server will receive updates and process clients. Another item to keep in mind is how many levels of servers you will have in a WSUS server hierarchy. Microsoft recommends not having more than three levels. Theoretically, you can have unlimited levels—but three would be adequate, any more and you would have synchronization issues. The two different modes a WSUS server can be are:

- **Autonomous Mode** An upstream WSUS server shares updates with its downstream server or servers during synchronization, but not update approval status or computer group information. Downstream WSUS servers must be administered separately. Autonomous servers can also synchronize updates for a set of languages that is a subset of the set synchronized by their upstream server.
- **Replica Mode** An upstream WSUS server shares updates, approval status, and computer groups with its downstream server or servers—these servers would be termed downstream replica servers.

### **EXAM WARNING**

When setting up WSUS 3.0 SP1, you will have an opportunity to select the languages you want to support. If you select all languages—it is going to take up an enormous amount of space. There may be a question or two about troubleshooting WSUS 3.0 SP1 disk space. This is a classic reason for losing a significant amount of disk space.

### **TEST DAY TIP**

On the exam, remember that Microsoft is going to use their terminology on the questions. For example: A question will refer to WSUS Server A in Figure 3.7 as the Upstream Server. This is important because the question may or may not have a drawing to refer to for the question. Make it a practice to learn the new terminology.

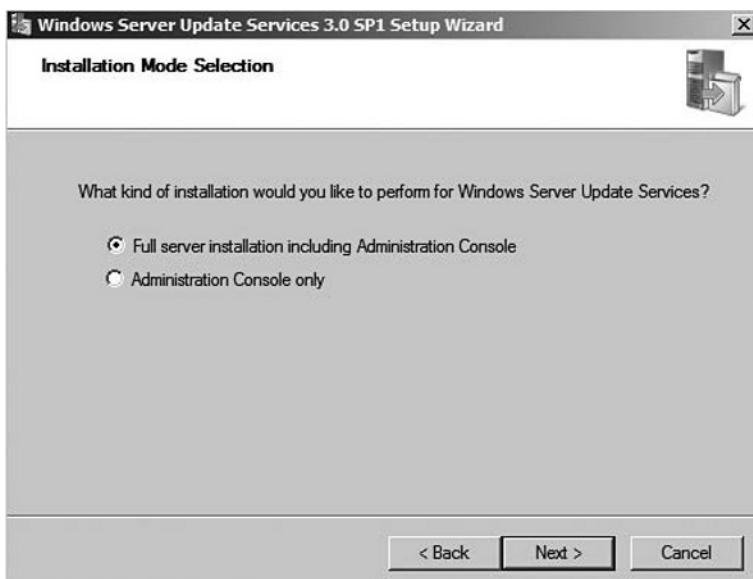
## EXERCISE 3.3

### INSTALLING WSUS SERVER 3.0 SP1

In this exercise, we are going to do a new installation of WSUS Server 3.0 SP1 on our test server. This exercise assumes you already have IIS 7.0 installed and configured per Exercise 3.2 instructions. If you don't have IIS 7.0 installed and configured—please go back and do Exercise 3.2. Also, download WSUS Server 3.0 SP1 (<http://go.microsoft.com/fwlink/?LinkId=88321>) and the Microsoft Report Viewer Redistributable 2005 (<http://go.microsoft.com/fwlink/?LinkId=70410>). Store these downloads on the desktop of the server.

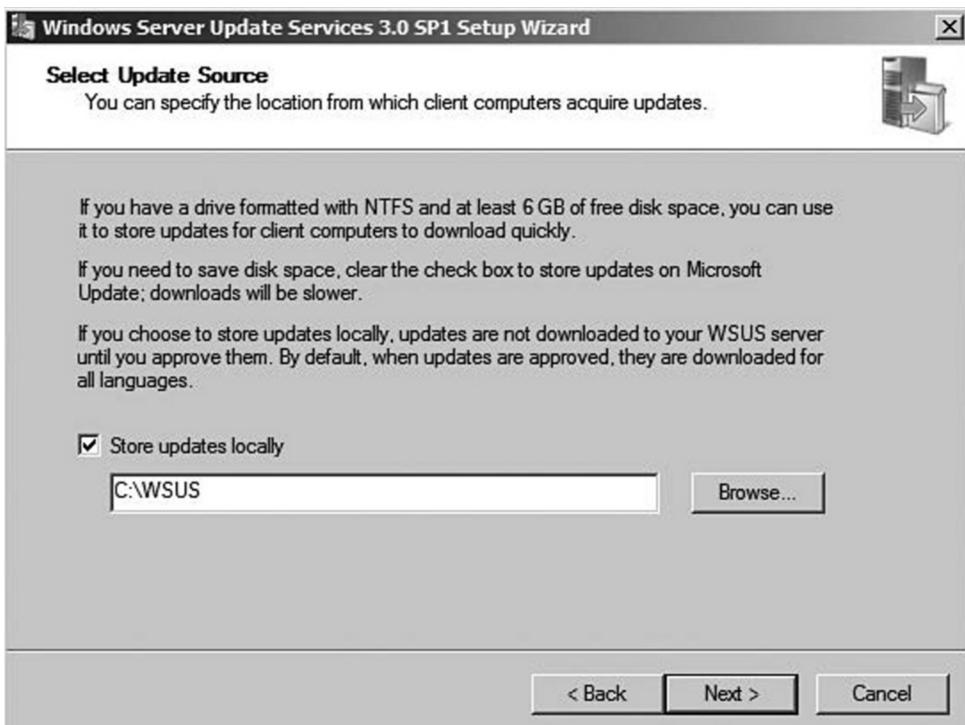
1. Double click the WSUS 3.0 SP1 installer on the desktop to start the installation. The name of the installer file is **WSUSSetup\_30SP1\_x86.exe**.
2. When the security dialog box comes up, click **Run** to start the installation.
3. The **Windows Server Update Services 3.0 SP1 Setup Wizard** appears on the screen. Click **Next** to continue the installation.
4. The **Installation Mode Selection** screen appears next. Make sure that **Full server installation including Administration Console** is selected (see Figure 3.8). Click **Next** to continue the installation.

**Figure 3.8** Installation Mode Selection

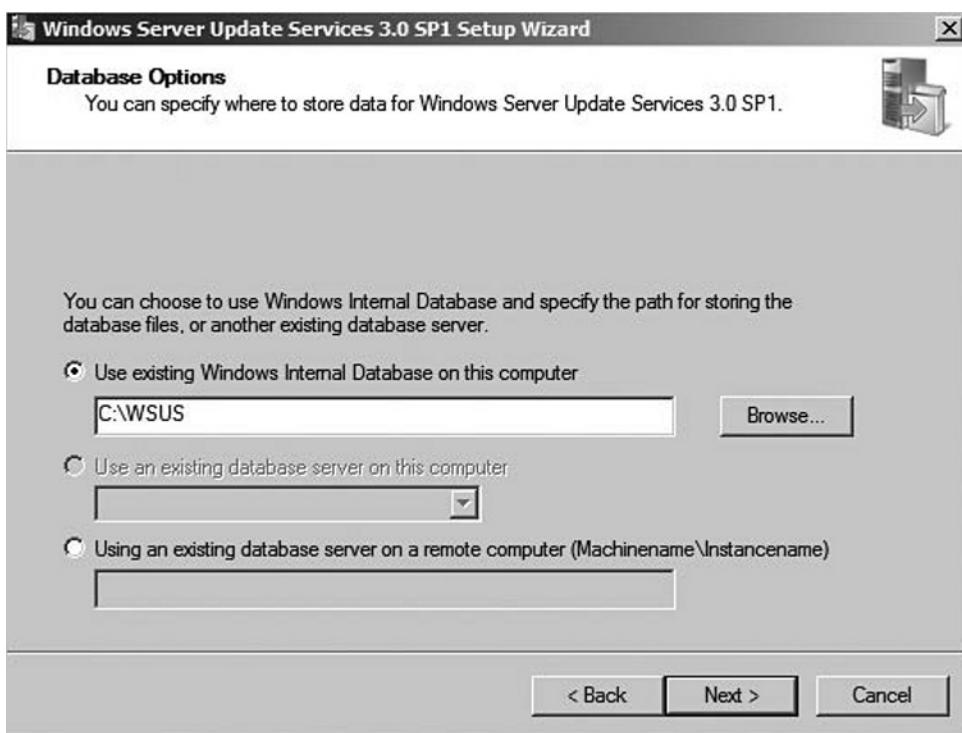


5. At the next screen, select **I accept the terms of the License agreement** and click **Next**.
6. The installer warns us that Microsoft Report Viewer 2005 Redistributable is not installed. We will install this after installing WSUS 3.0 SP1. Click **Next** to continue.
7. Next, we will need to select the place where we want to store the WSUS updates. Accept the default location as shown in Figure 3.9 and click **Next**.

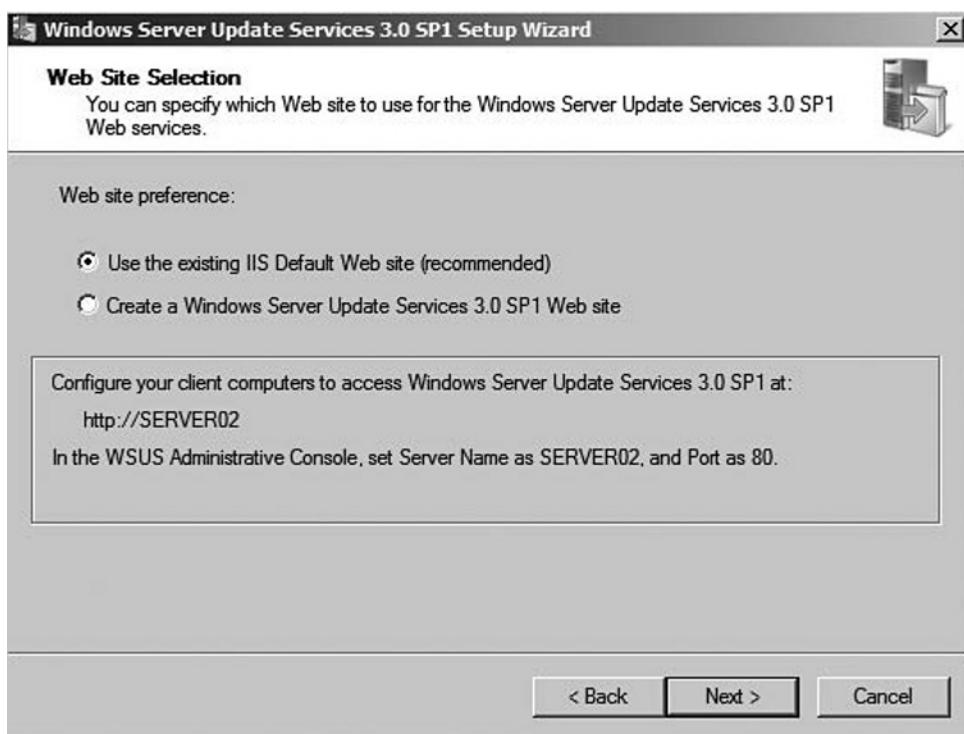
**Figure 3.9** Select Update Source



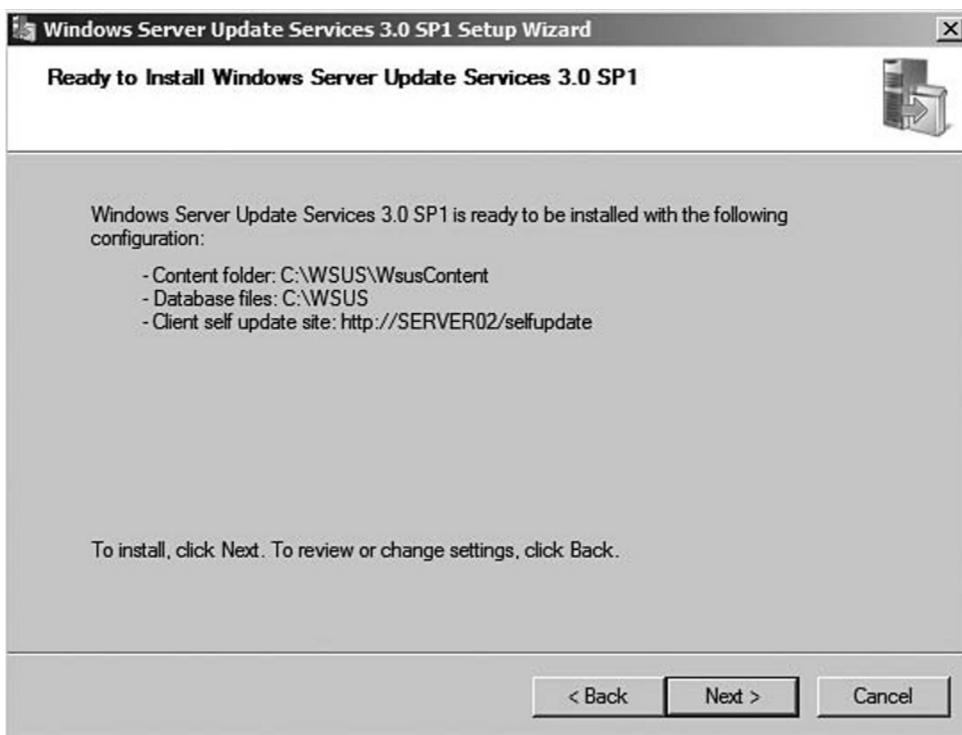
8. At the **Database Options** screen, we want to use the Windows internal database. Verify that **Use existing Windows Internal Database on this computer** is selected as shown in Figure 3.10 and click **Next**. Notice we can choose two other database options: **Use an existing database server on this computer** and **Using an existing database server on a remote computer (Machine\InstanceName)**. We can choose to use a standalone Microsoft SQL Server—if you choose this option, you must run Microsoft SQL Server 2005 Service Pack 1.

**Figure 3.10** Database Options

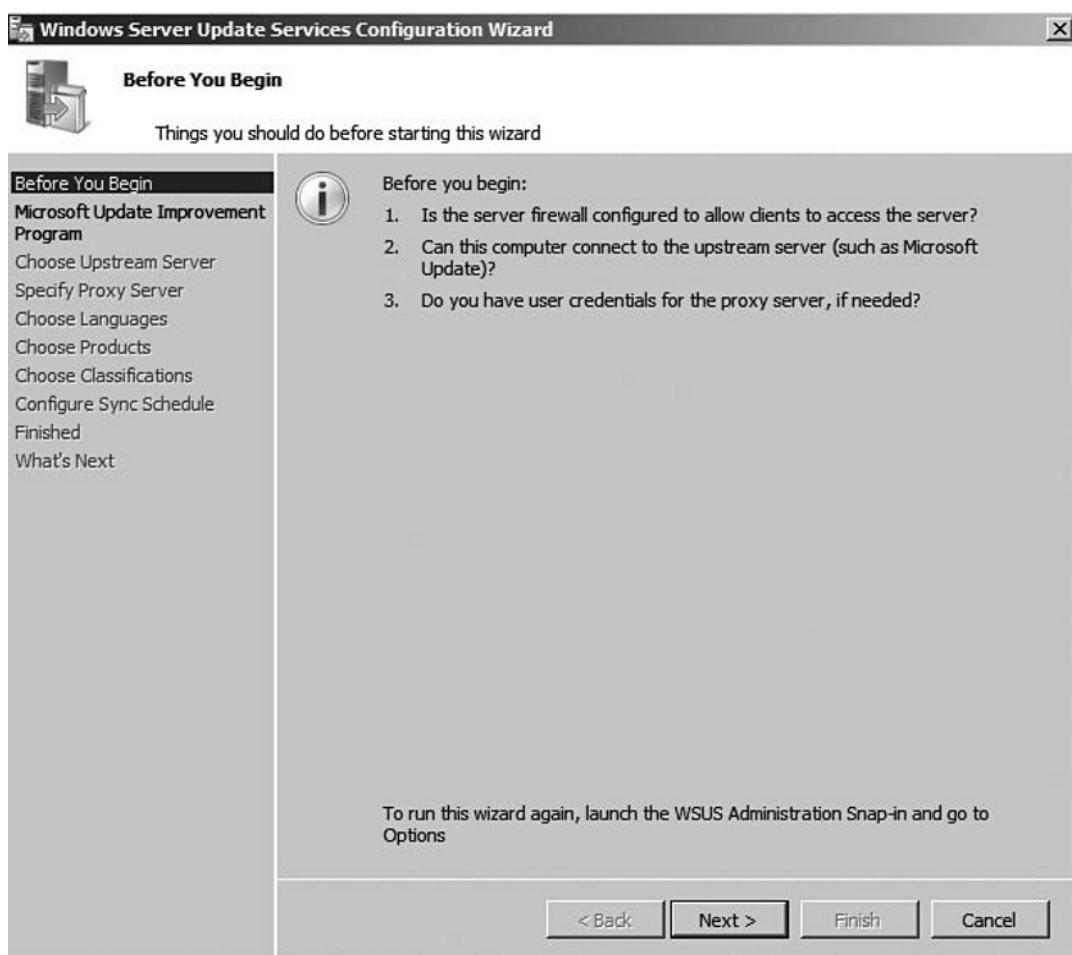
9. The installation will next create a Microsoft SQL Server Instance and connect to it. Note that the server uses Microsoft SQL Server 2005 Express to create the WSUS database. Once the server is **Successfully connected to SQL server instance**, click **Next**.
10. At the **Web Site Selection** screen, make sure that **Use the existing IIS Default Web site (recommended)** is selected, see Figure 3.11. Note we can change the port number or **Create a Windows Server Update Services 3.0 SP1 Web site**. Also, make note to the **Configure your client computers to access Windows Server Update Services 3.0 SP1 at**—this is the setting client computers will use to get updates. Click **Next** to continue with the installation.

**Figure 3.11** Web Site Selection

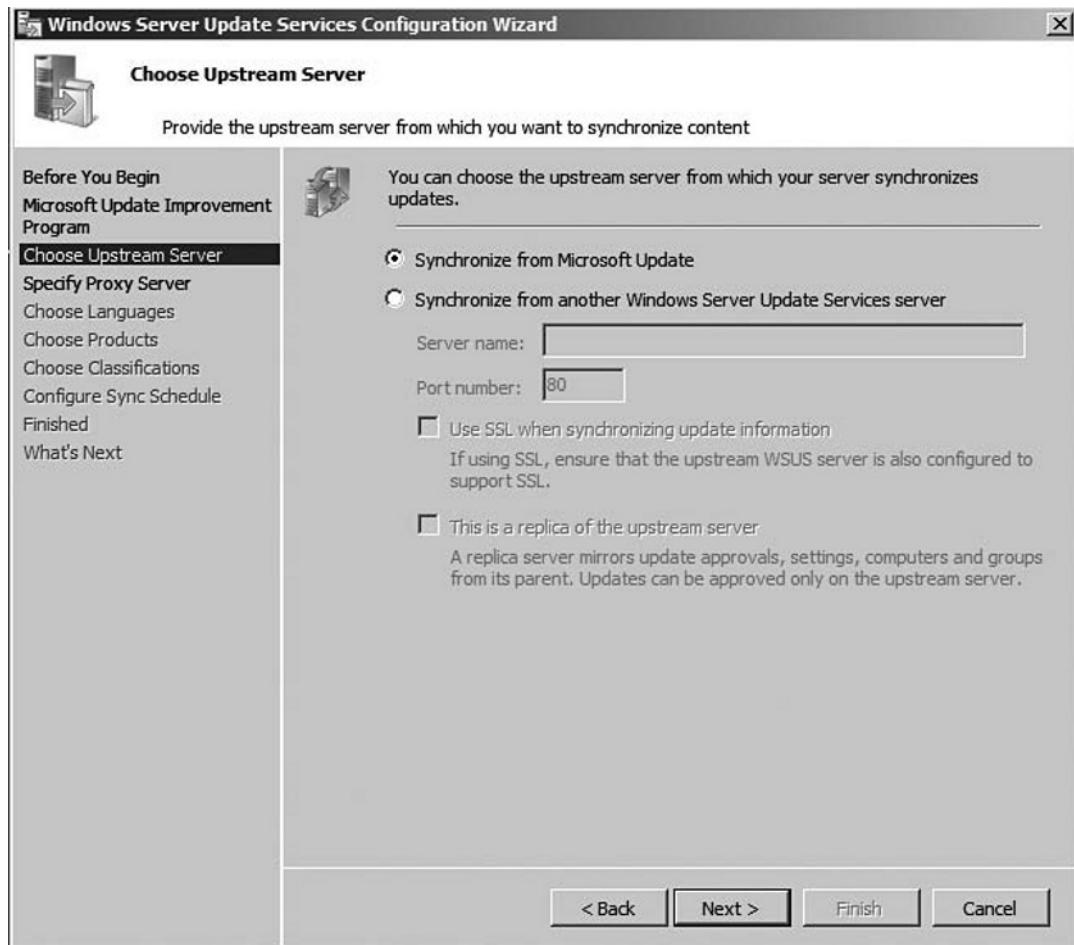
11. At the next screen, **Ready to Install Windows Update Services 3.0 SP1**, you have the opportunity to look over your configuration one last time before the installation. See Figure 3.12 and make sure your settings conform to the settings in the book (your server name may be different). Click **Next** to begin the installation of the files.

**Figure 3.12** Ready to Install Windows Server Update Services 3.0 SP1

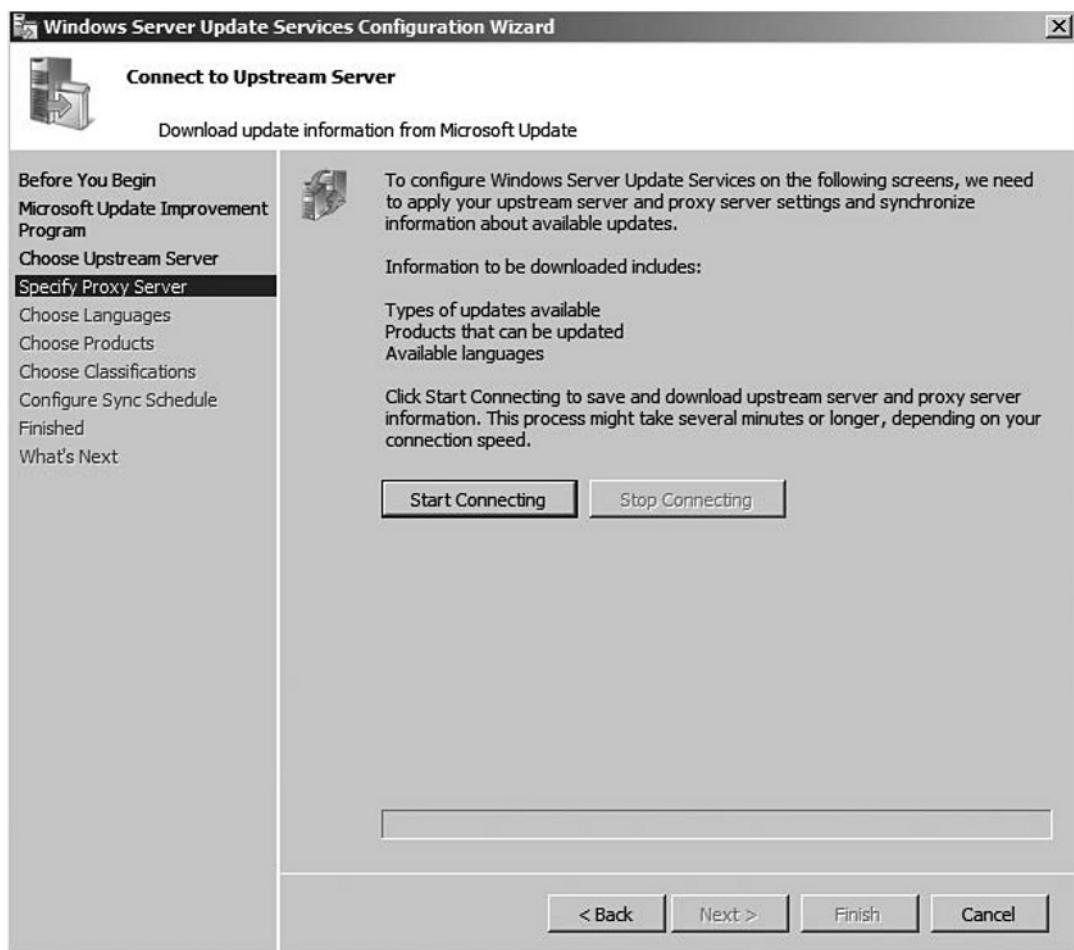
12. After the installation completes successfully, the **Completing the Windows Server Update Services 3.0 SP1 Setup Wizard** windows will appear. Make sure the box says **You have successfully completed the Windows Server Update Services 3.0 SP1 Setup Wizard**. Click **Finish** to complete the installation.
13. Microsoft has made configuring WSUS 3.0 SP1 easier to configure than previous versions. After the installation, the **Windows Server Update Services Configuration Wizard** starts automatically—see Figure 3.13. Click **Next** to begin the **Windows Server Update Services Configuration Wizard**.

**Figure 3.13** Windows Server Updates Services Configuration Wizard

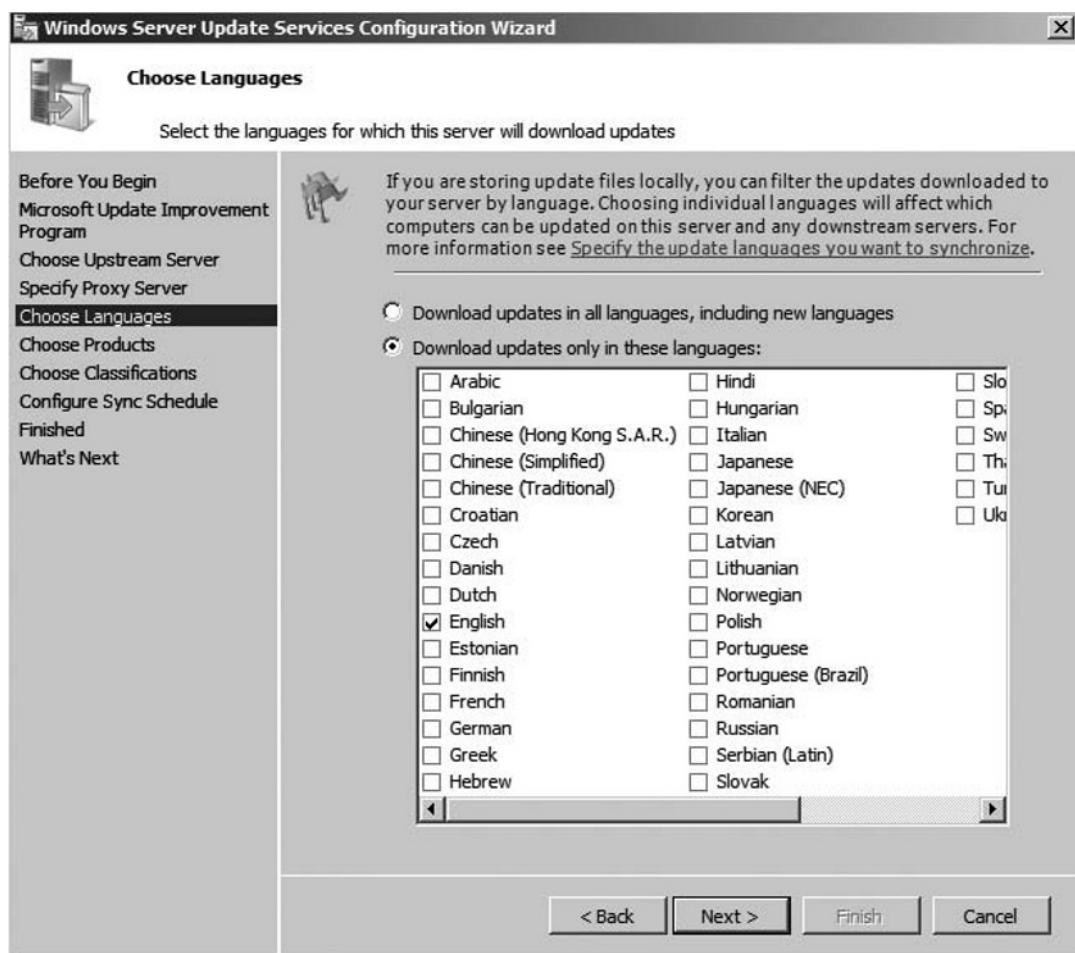
14. At the **Join the Microsoft Update Improvement Program**—click **Next** to accept the default settings.
15. The **Choose Upstream Server** window appears. Since this is our first WSUS server in the hierarchy—we need to make sure the **Synchronize from Microsoft Update** is selected. Note we can choose to update our WSUS server from another upstream WSUS server in our network by selecting **Synchronize from another Windows Server Update Services server**—see Figure 3.14. Click **Next** to proceed forward.

**Figure 3.14** Choose Upstream Server

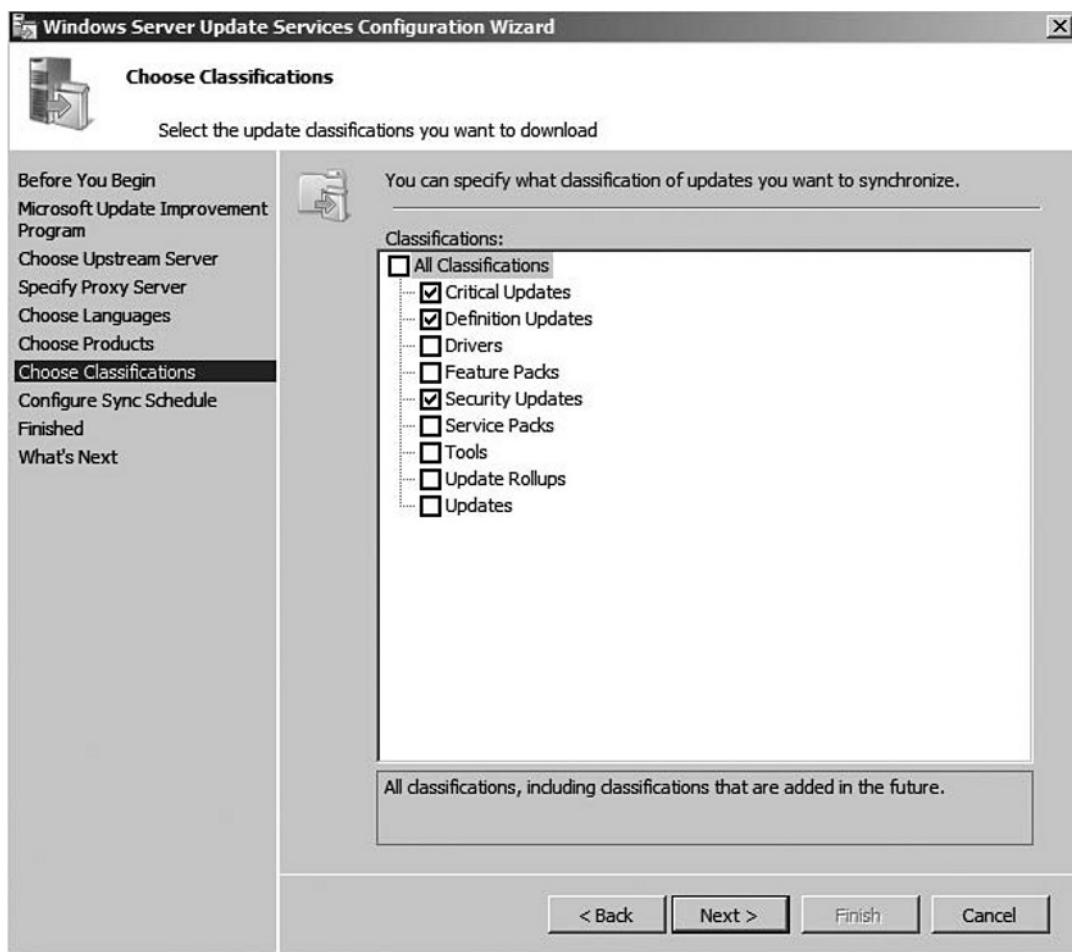
16. At the **Specify Proxy Server**, accept the default settings and click **Next** since we have no proxy server that needs configured.
17. Now we need to **Connect to Upstream Server**. This will download configuration information to choose what products our WSUS server will support. See Figure 3.15. Click **Start Collecting** to start downloading upstream server information.

**Figure 3.15** Connect to Upstream Server

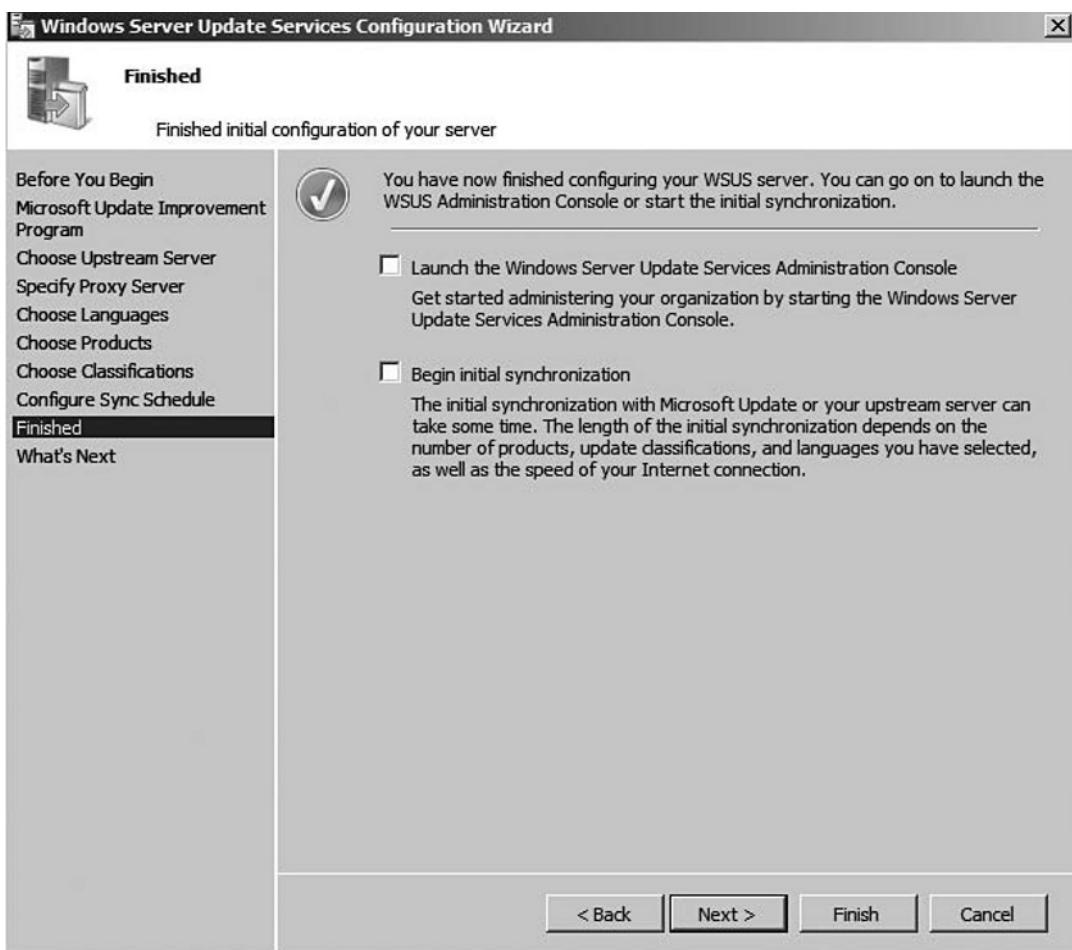
18. After the WSUS is done connecting, click **Next** to continue.
19. At the **Choose Languages** screen, make sure only English is selected and click **Next** (see Figure 3.16). If you must choose other languages in a production environment, remember that the size of your downloads will increase dramatically.

**Figure 3.16** Choose Languages

20. Now we will need to choose the products we would like to support with our WSUS installation. Accept the default settings and click **Next**.
21. The next screen, **Choose Classifications**, lets us choose the type of updates we would like to download from the upstream server—see Figure 3.17. Accept the defaults and click **Next**.

**Figure 3.17** Choose Classifications

22. Normally, we would **Set Sync Schedule** to perform downloads automatically at non-peak times during the day. For our exercise, we are going to leave the default at **Synchronize manually** and click **Next** to continue.
23. Unselect **Launch the Windows Server Update Services Administration Console** and **Begin initial synchronization** in the **Finished** window—see Figure 3.18. Click **Next** to continue.

**Figure 3.18** Finished

24. At the **What's Next** screen, click **Finish**.
25. Now that WSUS 3.0 SP1 installed—we still need to install the **Microsoft Report Viewer Redistributable 2005**. Double click the **ReportViewer.exe** icon on your desktop. This is the file we downloaded earlier—if you need to download the program, you can download it here: <http://go.microsoft.com/fwlink/?LinkId=70410>.
26. When the security dialog box comes up, click **Run** to start the installation.
27. At the **Welcome to Microsoft Report Viewer Redistributable 2005 Setup** screen, click **Next** to continue.

28. At the next screen, select **I accept the terms of the License agreement** and click **Install**.
  29. Once the setup is complete, click the **Finish** button to end this exercise.
- 

## Microsoft WSUS 3.0 Service Pack 1 Administration Console

A new feature that Microsoft added to WSUS 3.0 SP1 is the ability to manage WSUS from a Microsoft Management Console (MMC). This is called a Console Only installation. Older versions of WSUS relied on Internet Explorer and could be troublesome sometimes. With the new MMC, we have the ability to remotely manage a WSUS server or servers from the desktop of a regular PC. Operating systems that are supported for the WSUS 3.0 SP1 MMC include:

- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows XP Service Pack 2

Also, a Console Only installation has the following software prerequisites:

- Microsoft .Net Framework Version 2.0 Redistributable Package (<http://go.microsoft.com/fwlink/?LinkId=68935>)
- Microsoft Management Console 3.0 for Windows Server 2003 (<http://go.microsoft.com/fwlink/?LinkId=70412>)
- Microsoft Report Viewer Redistributable 2005 (<http://go.microsoft.com/fwlink/?LinkId=70410>)



### TEST DAY TIP

Make sure on the day of the exam that you know minimum software requirements for different features, roles, and other software installations. Microsoft likes to ask questions that draw from whether or not you understand software minimum requirements—this can also include minimum hardware requirements.

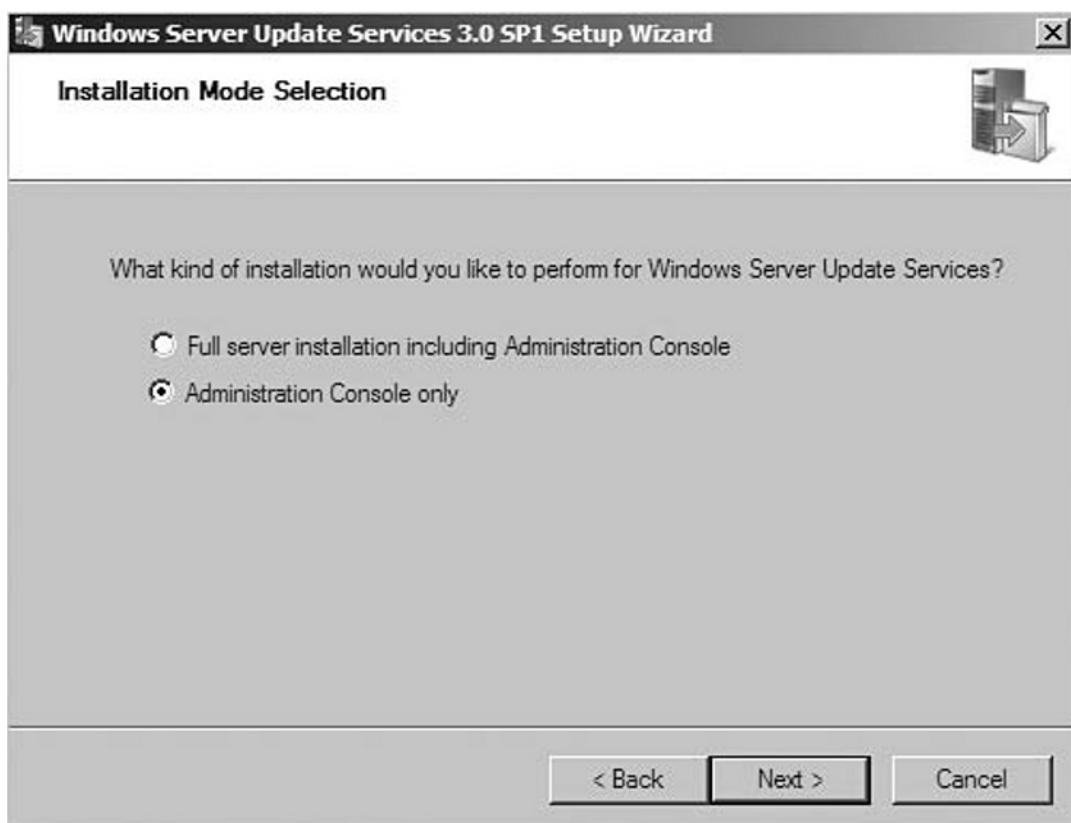
## EXERCISE 3.4

### MICROSOFT WSUS 3.0 SERVICE PACK 1 CONSOLE ONLY INSTALLATION

In this exercise, we are going to perform a Console Only installation or WSUS 3.0 SP1 on a Microsoft Windows 2008 Server. Also, we are going to connect it to the server we originally installed in Exercise 3.3. For this exercise, you will need the server that we installed WSUS on in Exercise 3.3 and a second server. This is where Microsoft Virtual PC 2007 will be very useful when practicing the exercises.

1. Download Microsoft WSUS 3.0 SP1 and the Microsoft Report Viewer Redistributable 2005 to the desktop of your second server.
2. Double-click **WSUSSetup\_30SP1\_x86.exe** on the desktop to start the WSUS installation.
3. When the security dialog box comes up, click **Run** to start the installation.
4. The **Windows Server Update Services 3.0 SP1 Setup Wizard** appears on the screen. Click **Next** to continue the installation.
5. The **Installation Mode Selection** screen appears next. Make sure that **Administration Console only** is selected. See Figure 3.19. Click **Next** to continue the installation.

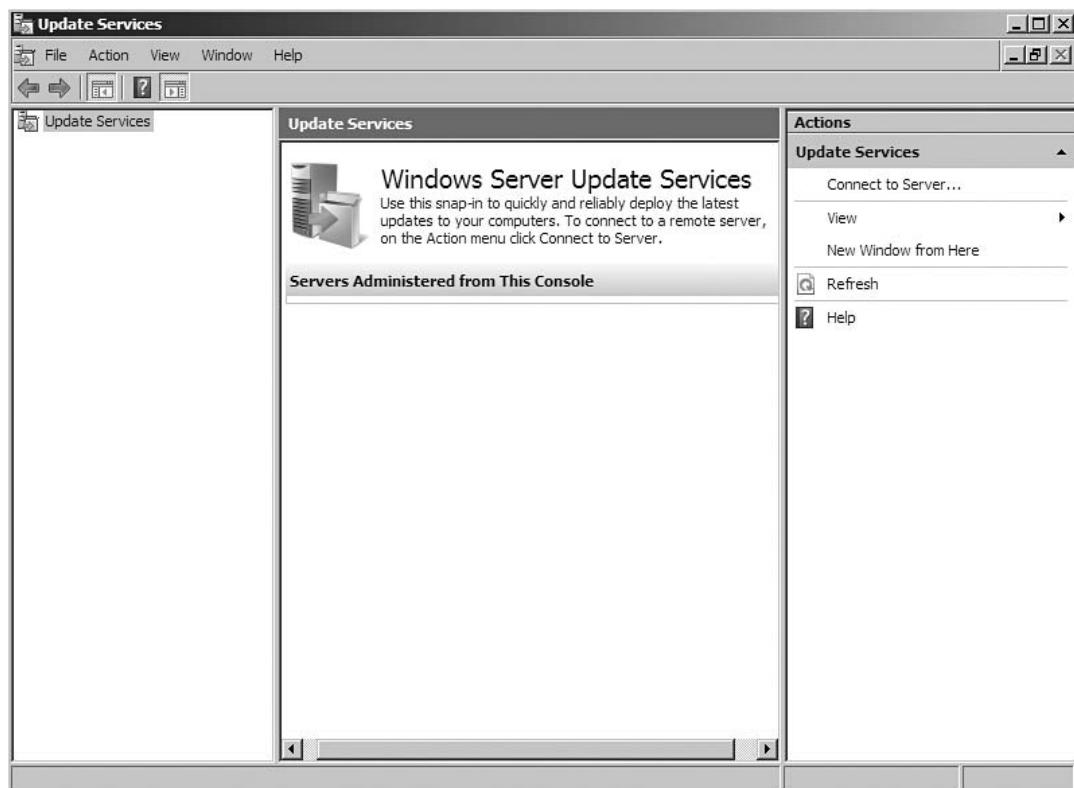
**Figure 3.19** Installation Mode Selection



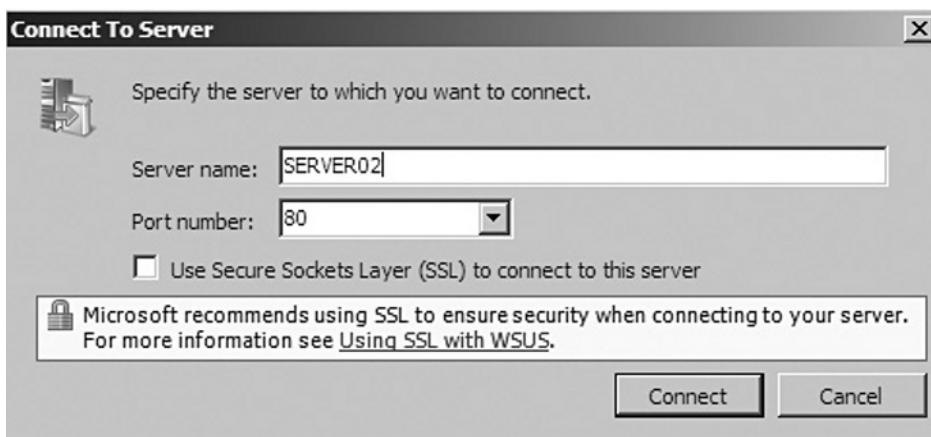
6. At the next screen, select **I accept the terms of the License agreement** and click **Next**.
7. The installer warns us that **Microsoft Report Viewer 2005 Redistributable** is not installed. We will install this after installing WSUS 3.0 SP1 Administration Console. Click **Next** to continue.
8. At the next screen, click **Finish** to complete the installation.
9. Now that WSUS 3.0 SP1 Administration Console is installed—we still need to install the **Microsoft Report Viewer Redistributable 2005**. Double click the **ReportViewer.exe** icon on your desktop. This is the file we downloaded earlier—if you need to download the program, you can download it here: <http://go.microsoft.com/fwlink/?LinkId=70410>.
10. When the security dialog box comes up, click **Run** to start the installation.

11. At the **Welcome to Microsoft Report Viewer Redistributable 2005 Setup** screen, click **Next** to continue.
12. At the next screen, select **I accept the terms of the License agreement** and click **Install**.
13. Once the setup is complete, click the **Finish** to exit the installation.
14. Click **Start | Administrative Tools | Microsoft Windows Server Update Services 3.0 SP1**. This starts the WSUS Console—see Figure 3.20.

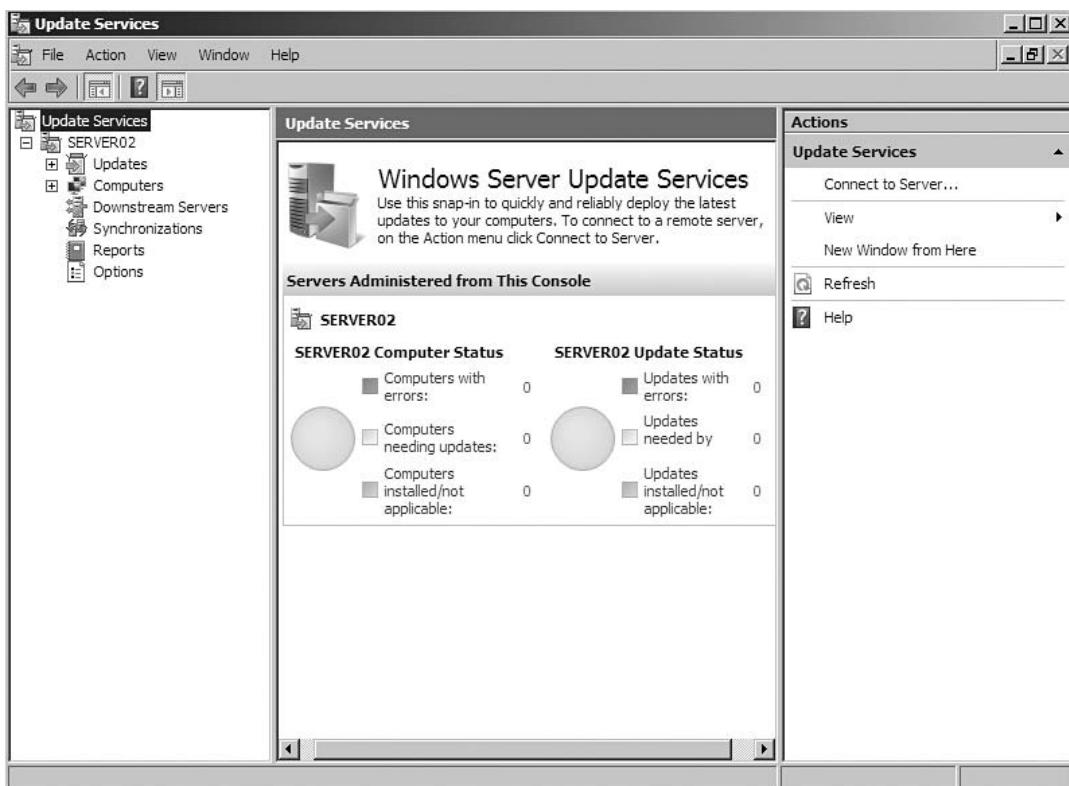
**Figure 3.20** Update Services



15. On the right pane in the **Update Services Console**, click **Connect to Server**. A dialog box will come up and ask which server you would like to connect to—in my example, I want to connect to SERVER02 (your server may be a different name). Enter Server02 in the dialog box. See Figure 3.21. Then click **Connect**.

**Figure 3.21** Connect to Server

16. You are now connected to SERVER02 with the WSUS Management Console. Your MMC should look like Figure 3.22.

**Figure 3.22** Update Services Management Console

17. Click **File** then **Exit** to close the WSUS MMC Console.

### EXAM WARNING

Be very sure to familiarize yourself with the different options and selections within the WSUS Console MMC. Some questions may ask you to perform a task—it will be necessary for you to understand where different commands and options reside inside of the WSUS Console MMC.

### New and Noteworthy...

#### Secure Connection to Microsoft Windows Server Update Services

As seen previously in this chapter in Figure 3.21, Microsoft recommends using HTTPS to connect to the Microsoft Windows Server Update Services server for management. HTTPS is secured because it uses the SSL (Secured Socket Layer) protocol. From my experience, I have seen a lot of seasoned administrators ignore this suggestion and proceed to use HTTP to manage the server.

SSL encrypts all data being transferred from the Microsoft WSUS server, including password information and all data you see on your Microsoft Management Console when connected to the WSUS server. The information is secured with certificates—before you think you need to go out and purchase a certificate from Verisign to manager your WSUS server remotely, you don't. The easiest solution is to use the Microsoft Directory Certificate Services role on a Microsoft Windows 2008 Server to create a certificate for your private network.

By securing your connection with the Microsoft WSUS server, you will prevent many possible security breaches. Using a SSL certificate can help prevent violators from obtaining private information from network because all of the data is encrypted. Also, with using certificates—the connector can be verified with use of certificates. As you can see—using SSL should not be overlooked when configuring a connection to a Microsoft WSUS server, or for any server service for that matter.

## Configure Microsoft WSUS 3.0 Service Pack 1 Automatic Updates for Clients

Once WSUS 3.0 SP1 is installed, we need to configure the clients to receive automatic updates from the WSUS server. Automatic Updates is the client component of WSUS 3.0 SP1. There are a couple different ways to do this, but the majority of administrators will choose to use the Group Policy Object with Active Directory to push down the settings. If you happen to be working on a network that does not have Active Directory installed, you can use the Local Group Policy Object on the client computer to point it at a WSUS server to obtain updates. This could get messy in a rather large network. Active Directory Group Policy Object is the easiest and most efficient way to push down the settings. WSUS 3.0 SP1 can push automatic updates to the following operating systems:

- Microsoft Windows Vista
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003, all versions and service packs
- Microsoft Windows XP Professional, Service Pack 1 or Service Pack 2
- Microsoft Windows 2000 Professional Service Pack 4, Microsoft Windows 2000 Server Service Pack 4 or Microsoft Windows 2000 Advanced Server Service Pack 4

### Configuring & Implementing...

#### Other Ways to Configure Clients to Receive Updates from a WSUS Server

The best way to push down Microsoft WSUS settings to client computers is by using Microsoft Active Directory Services if your systems are in a domain or by using the Local Group Policy Object if your workstations are located on a workgroup. There are some other ways to push down these settings if you need to do it in some other fashion.

The easiest way would be to create a Registry File called `WSUS_Update.reg` to import into your clients, adjusting the settings to correct

Continued

values for your network. Place this file in the root of your systems drive. The following is an example of a registry file to create these settings:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
    "WUServer"="http://YOUR-WSUS-SERVER"
    "WUStatusServer"="http://YOUR-WSUS-SERVER"
    "TargetGroupEnabled"=dword:00000001
    "TargetGroup"="Change Group"
    "ElevateNonAdmins"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]
    "NoAutoUpdate"=dword:00000000
    "AUOptions"=dword:00000004
    "ScheduledInstallDay"=dword:00000000
    "ScheduledInstallTime"=dword:0000000a
    "NoAutoRebootWithLoggedOnUsers"=dword:00000001
    "AutoInstallMinorUpdates"=dword:00000001
    "RebootRelaunchTimeoutEnabled"=dword:00000001
    "RebootRelaunchTimeout"=dword:0000003c
    "RescheduleWaitTimeEnabled"=dword:00000001
    "RescheduleWaitTime"=dword:0000000f
    "DetectionFrequencyEnabled"=dword:00000001
    "RebootWarningTimeoutEnabled"=dword:00000001
    "RebootWarningTimeout"=dword:0000001e
    "UseWUServer"=dword:00000001
    "NoAUSHutdownOption"=dword:00000000
    "NoAUAsDefaultShutdownOption"=dword:00000000
```

In this example, you would need to change the TargetGroup to match your environment settings. Also, the WUServer and WUStatusServer would need to be changed to your Microsoft WSUS server. I put these setting in bold type face above to help you find them. You could easily go to each workstation and import this file into each workstation's registry. I would recommend using a script file instead and use it to import the registry file and restart the Windows Update service on the client workstation. You would need to create the script with a CMD or BAT extension to run

Continued

properly. An example script is below—this script assumes the registry file WSUS\_Update.REG is in the root of the systems drive:

```
Net Stop "wuauserv"  
Echo Importing WSUS_Update.REG  
%windir%\Regedit.exe /s C:\WSUS_Update.REG  
Echo WSUS.reg imported successfully  
Net Start "wuauserv"
```

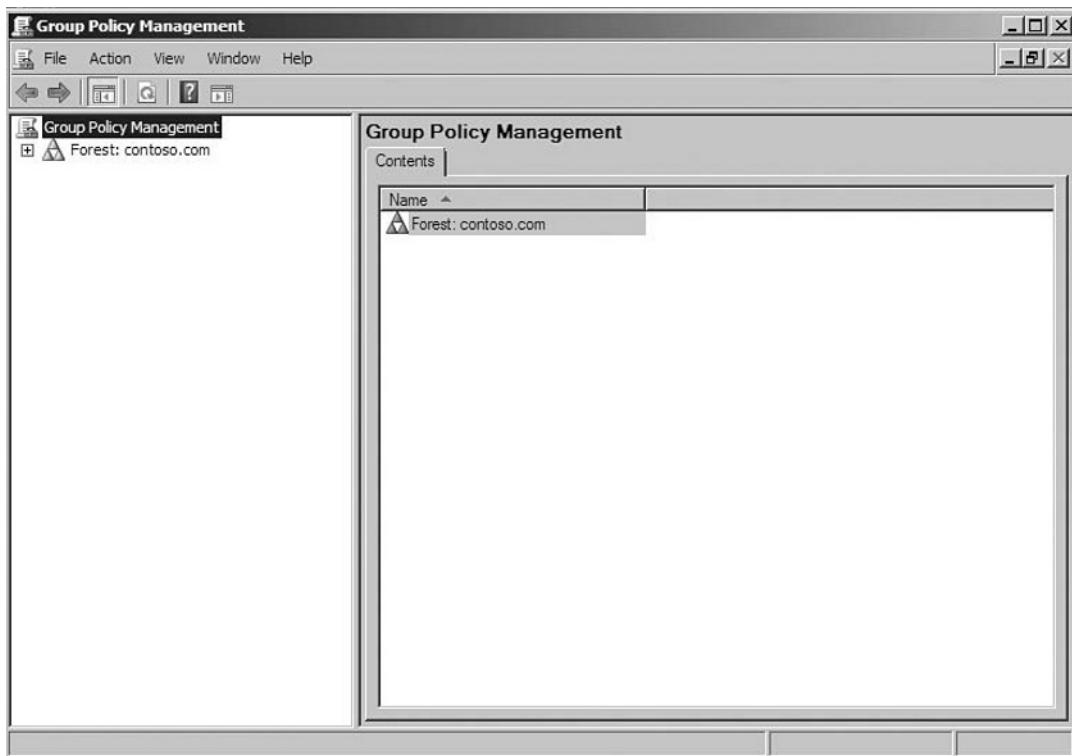
As you can see, there are other ways to change the WSUS settings on a client without using Active Directory Group Policy Objects or Local Group Policy Objects.

## EXERCISE 3.5

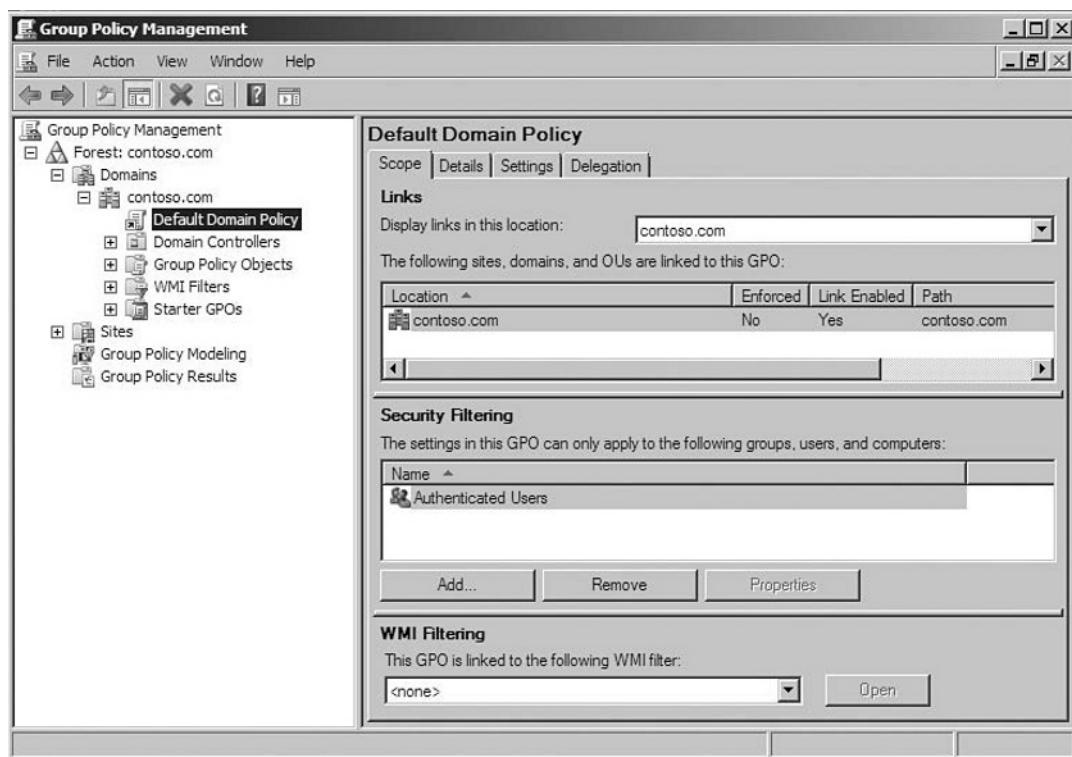
### CONFIGURING ACTIVE DIRECTORY TO PUSH SETTINGS DOWN TO CLIENTS FOR MICROSOFT WSUS 3.0 SERVICE PACK 1

In this exercise, we are going to configure our Active Directory controller to use Group Policy Object to push down WSUS settings to the client. To do this, we will not need to add the WSUS Administrative Template to the Group Policy Object—Microsoft Windows Server 2008 already has it installed by default. Just configure Automatic Updates and point the clients to the WSUS server. For this exercise, we are going to edit the Default Domain Policy. This would push settings down to all computers and server in the Active Directory.

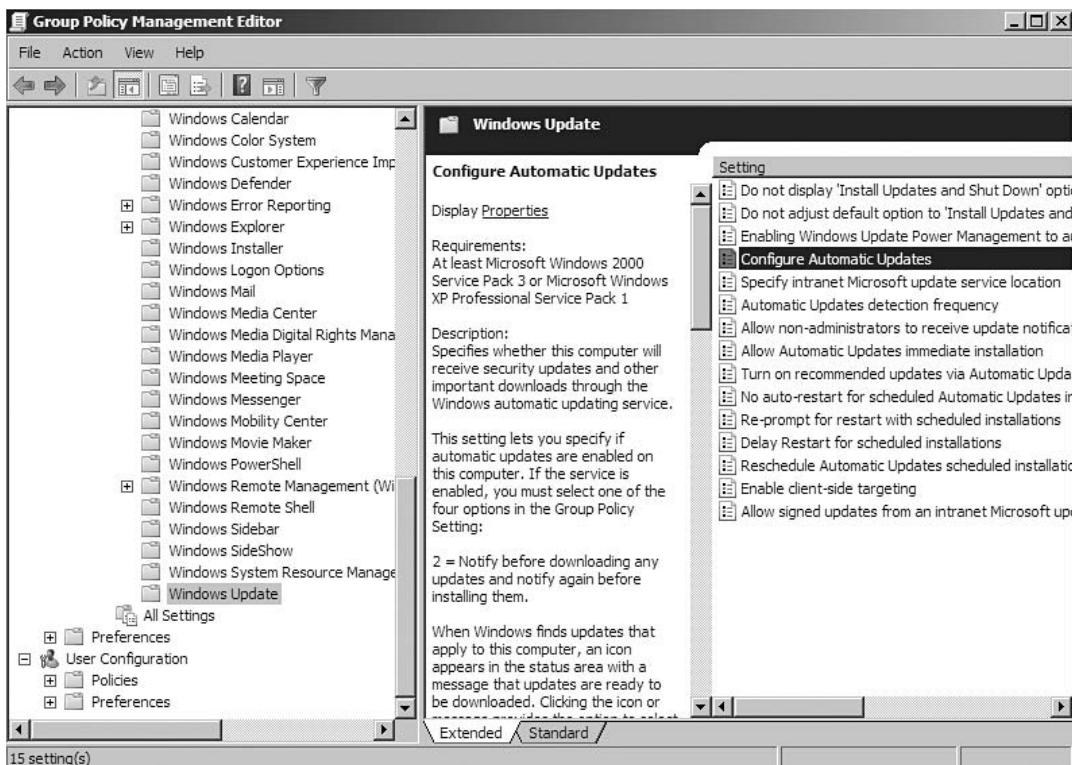
1. Click Start | Administrative Tools. Open the **Group Policy Management** as seen in Figure 3.23.

**Figure 3.23 Group Policy Management**

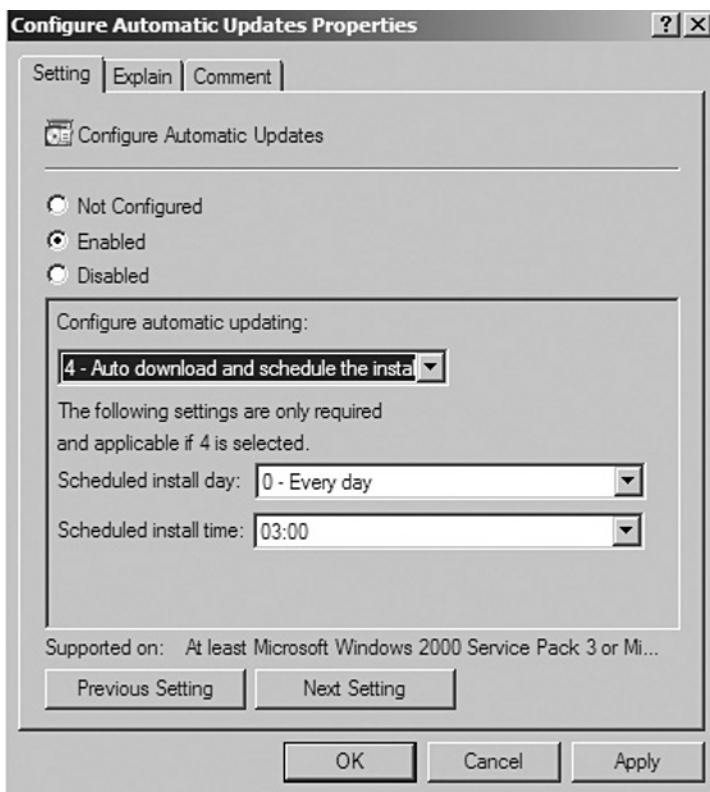
2. Expand the **Forest: Contoso.Com** domain. Note: Your domain name may be different. Underneath **Forest: Contoso.Com**, expand the **Domain** folder. Then, expand the **Contoso.Com** folder.
3. Select the **Default Domain Policy**. A dialog box will appear: **You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO and will impact all other locations where this GPO is linked.** Select **OK** to continue. At this point, your Group Policy Management console should look like Figure 3.24.

**Figure 3.24** Group Policy Management

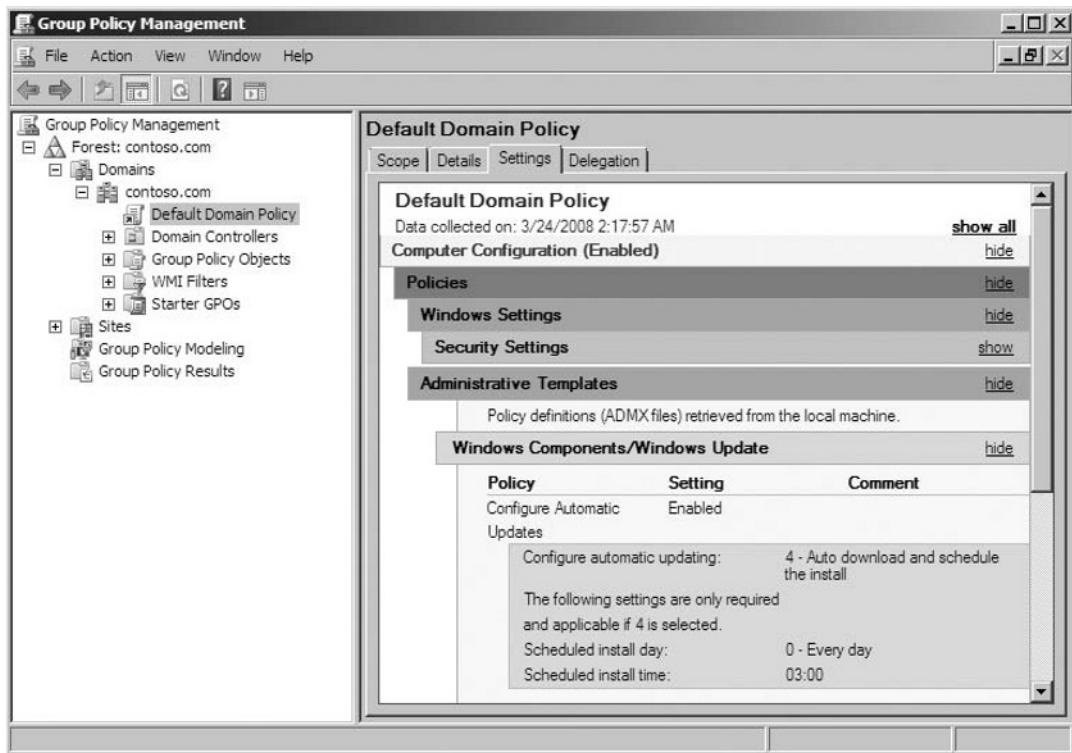
4. Right-click Default Domain Policy and select **Edit**.
5. Under Computer Configuration, expand **Policies**, **Administrative Templates**, and **Windows Components** then select **Windows Update**.
6. Double-click **Configure Automatic Updates** on the right-side pane. See Figure 3.25 for location of Automatic Updates.

**Figure 3.25** Group Policy Management Editor

7. Double-click **Configure Automatic Updates** in the right pane. A new window appears to allow you to change the settings.
8. For our example, we are going to select the following settings: Choose the **Enable** button. Under Configure automatic updating, choose option **4—Auto download and schedule the install**. The **Scheduled install day** should be **Every day** and the **Scheduled install time** should be **03:00**. See Figure 3.26 for the correct settings. Then click **OK**.

**Figure 3.26** Configure Automatic Updates Properties

9. Select **File** then **Exit** to close the Group Policy Management Editor.
10. In the Group Policy Management console, choose the **Setting** tab in the right pane. You should see the setting you just entered. Verify that the setting looks like those in Figure 3.27.

**Figure 3.27 Group Policy Management**

11. Click **File** then **Exit** to close the Group Policy Management console.

## Application Patching

Within Microsoft WSUS 3.0 SP1, Microsoft has a feature to allow us to update Microsoft-based products. This is very useful and makes application patch management very easy. Unfortunately, if you need to patch third party applications, you will need to invest in a more elaborate patch management solution—Microsoft Systems Center Essentials 2007 or System Center Configuration Manager 2007.

Patch management for applications is very similar to patch management for Microsoft operating systems. Updates need to be approved to make available to the clients. It is very important to test your application patches before pushing them down to production systems. WSUS gives you the ability to push updates to a subset of computers—for instance, maybe a test group before rolling out to production.

## Head of the Class...

### Patching Other Third-Party Applications

One of the topics that come up continuously in the classroom environment deals with the patching of third party applications. At this time, and unfortunately, Microsoft does not make the patching of third party applications available in Microsoft Windows Server Update Services. There are third party applications and software solutions available from Microsoft to support the installation and updates of third party applications.

The software solutions for Microsoft include two products. The first product is Microsoft System Center Essentials 2007. This product is intended to support up to 30 servers and 500 client workstations. Using the Microsoft System Center Essentials 2007 single console design, IT administrators can easily secure, update, monitor, and track their IT environment. In addition, Microsoft System Center Essentials 2007 comes with many predefined reports that display various types of information and preloaded Management Packs to help monitor common operating system components, services and applications.

In an enterprise environment that surpasses 30 servers and 500 clients, Microsoft makes available Microsoft System Center Configuration Manager 2007. It provides the same features as Microsoft System Center Essentials 2007, but includes other features such as: remote controlling computers, metering software usage, deploying operating systems, and collecting hardware and software inventory. As you can see, Microsoft System Center Configuration Manager 2007 is a very powerful management solution—it also can be complicated to first set up and configure.

## EXERCISE 3.6

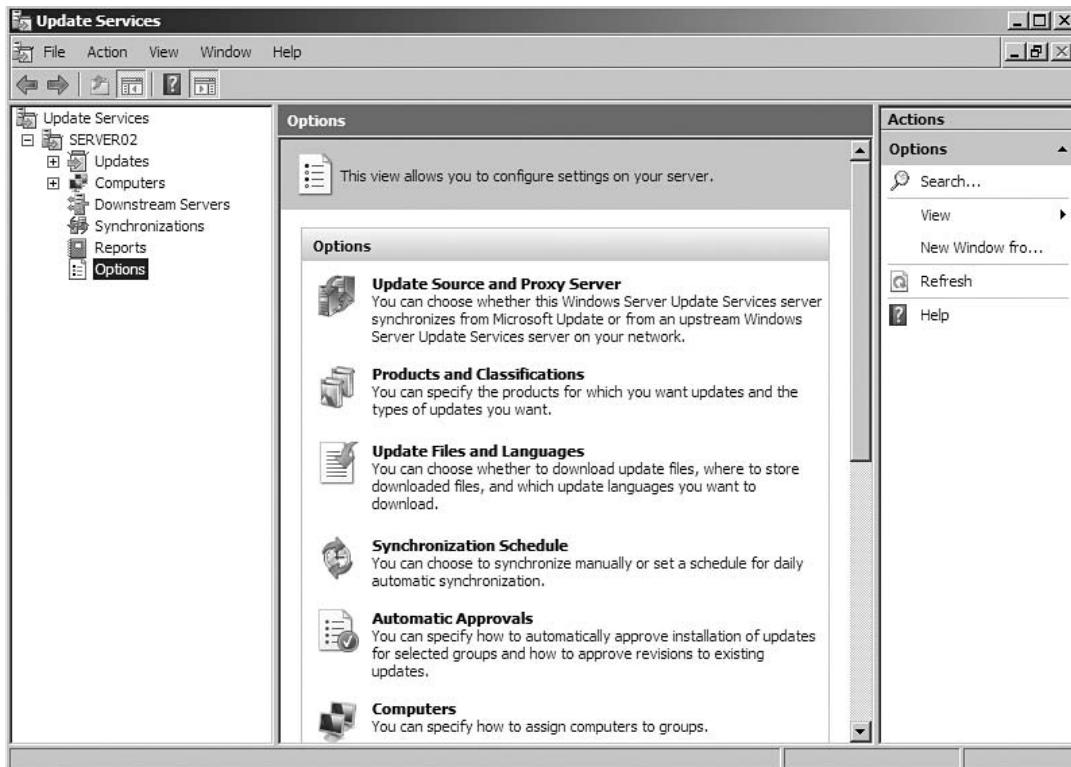
### SELECTING APPLICATIONS TO BE PATCHED IN MICROSOFT WSUS SERVICE PACK 1

In this exercise, we are going to verify that Microsoft WSUS is configured to update all versions of Microsoft Office and Microsoft Exchange Server 2007.

This exercise assumes you have the WSUS Console installed and connected to a WSUS server.

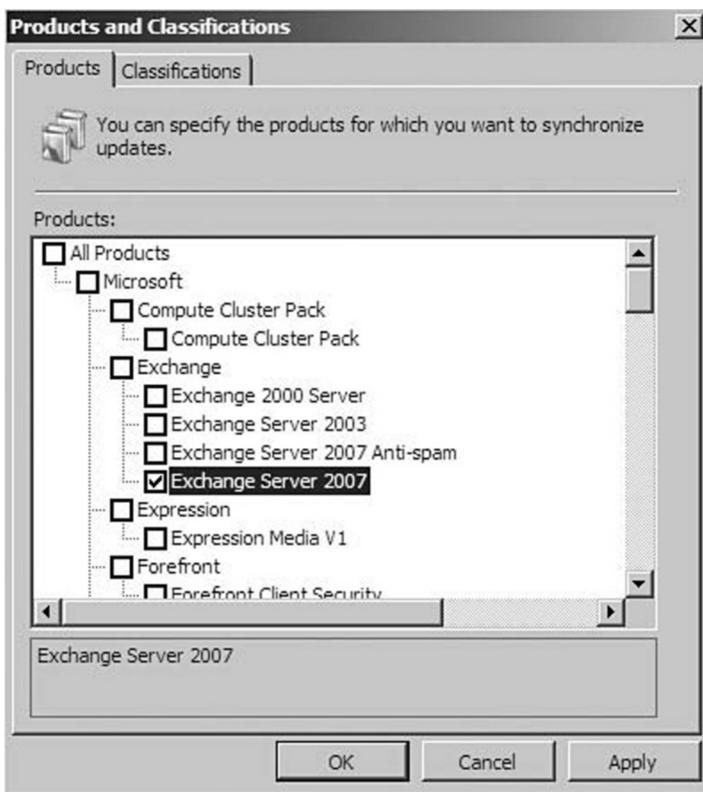
1. Click Start | Administrative Tools | Microsoft Windows Server Update Services 3.0 SP1.
2. On the left pane of the Microsoft WSUS Console, select the **Options** group at the bottom of the tree—you should see the same layout as in Figure 3.28.

**Figure 3.28** Update Services



3. Click on **Products and Classifications** in the middle pane.
4. In the **Products and Classifications** window, make sure all versions of **Microsoft Office** and **Microsoft Exchange Server 2007** are selected. See Figure 3.29.

### **Figure 3.29** Products and Classifications



5. Click **OK** to close the **Products and Classifications** screen.
  6. Click **File** then **Exit** to close the WSUS MMC Console.

# Monitoring for Performance

Monitoring servers for performance is very important to businesses. Most businesses are looking for cost effective solutions that let them get the most out of their IT investment. By monitoring the performance of our servers in the infrastructure, we have the ability to determine which servers are being over or under utilized. By identifying components requiring additional tuning, you are able to improve the efficiency of your servers. It is very important to plan proper server capacity planning, that way our hardware is used efficiently and in a way to help reduce overall costs. Monitoring our servers for performance also helps us keep the infrastructure free of

problems and allows the administrator to prevent future problems by identifying any potential issues before they become serious. Other key reasons to monitor server and service performance include:

- Health of the IT Infrastructure
- Service Level Agreement Monitoring
- Planning for Future Requirements
- Identifying Issues

### **EXAM WARNING**

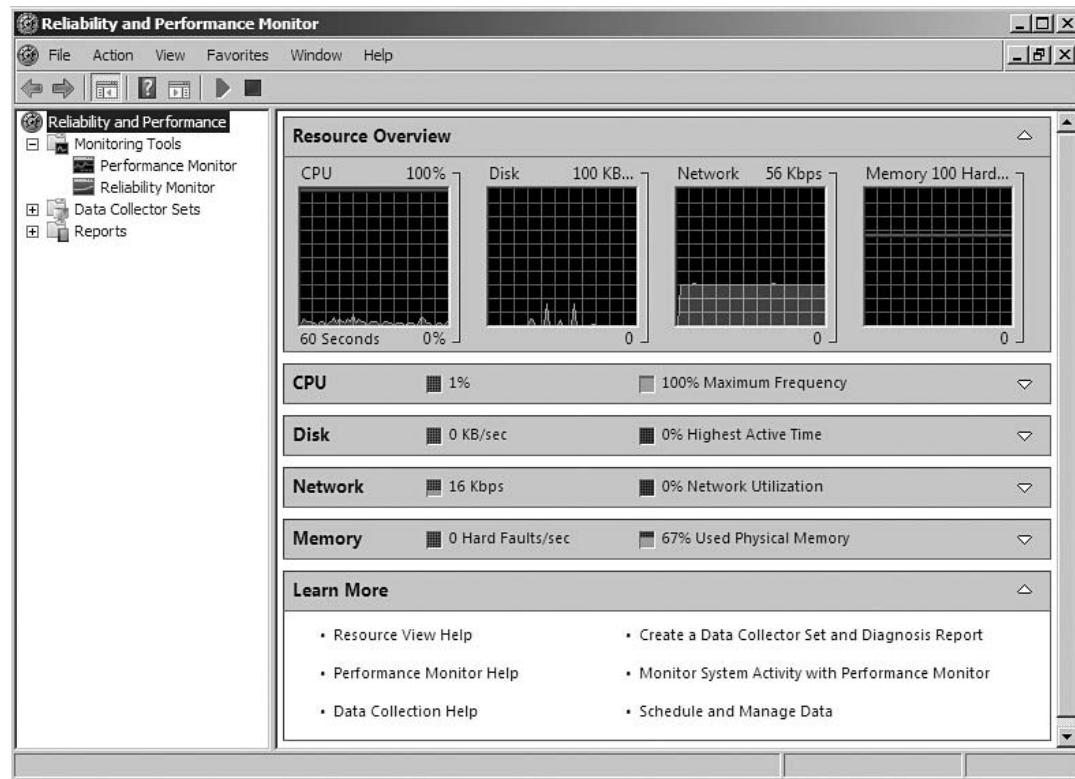
On the exam, it will be important to know how to monitor and collect performance data. Keep in mind, you may also be asked to interpret the data. For instance, you may be given values of a performance monitoring session. You may be asked how to correct a performance issue, such as: Does the server need more bandwidth? Is the memory capacity supporting the server work load? Remember to know how to collect data and also to interpret the information.

## **EXERCISE 3.7**

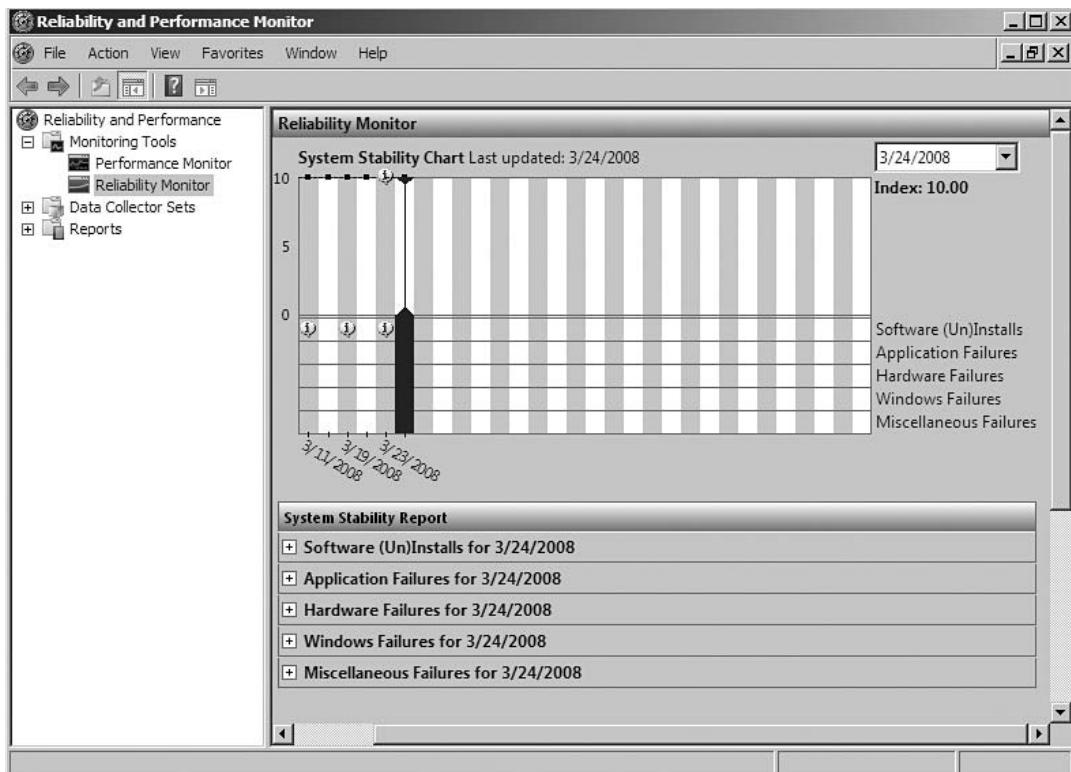
### **OPENING THE RELIABILITY AND PERFORMANCE MONITOR**

In this exercise, we are going to work with the Reliability and Performance Monitor. As you quickly will see, the Reliability and Performance Monitor in Microsoft Windows Server 2008 is very different than in previous versions of Microsoft Windows server editions.

1. Click Start | Administrative Tools | Reliability and Performance Monitor.
2. In the tree on the left pane, select Reliability and Performance at the top of the tree. See **Figure 3.30**.

**Figure 3.30 Reliability and Performance**

3. Click on **Performance Monitor**. Notice the Performance Monitor is still like previous versions of Windows Server editions. There are more counters available.
4. Click on **Reliability Monitor**. The Reliability Monitor gives us a System Stability Report, as seen in Figure 3.31.

**Figure 3.31 Reliability Monitor**

5. Click **File** then **Exit** to close the Reliability and Performance Monitor.

## Monitoring Servers

When monitoring servers, it is very important to use the appropriate tool to perform the monitoring functions. Basically, you should select the most appropriate tool to suit the type of monitoring required. The two main types of monitoring include historical and real time. Historical monitoring allows us to collect data over a set time frame—this data can be used at a later date to determine if the server needs more resources or why the system is performing poorly. Using collected data as empirical evidence of whether or not a server is performing poorly is more definitive than user perception. Performing real time monitoring is good when you need to figure out why a server is running poorly at a specific time—this is good to troubleshoot a problem.

Most of your monitoring of performance and reliability will take place in the new MMC Performance and Reliability Monitor. Microsoft has really improved this tool from the previous Microsoft Windows versions. The Reliability and Performance Monitor provides the IT professional with a quick, visual representation of the stability and performance of your system. In addition, it tracks events that will help you identify what causes reduction in stability and performance. New features include the following:

- **Data Collector Sets** Data collectors are grouped together into a set. Once they are grouped, they can be reusable. Also, we are able to take the Data Collector Sets and schedule them to run create logs and save as a template to use on other systems.
- **Wizards and Templates for creating logs** You can now add counters and log files and schedule their start, stop, and duration through a wizard interface.
- **Resource Overview** Provides real time graphical overview of CPU, disk, network, and memory usage. Refer back to Figure 3.30 to see the Resource Overview.
- **Microsoft Performance and Reliability Monitor** Calculates a System Stability Index that reflects whether unexpected problems reduced the reliability of the system. Refer back to Figure 3.31 to see the Reliability Monitor.
- **Unified property configuration for all data collection, including scheduling.**
- **User friendly diagnosis reports.**

The Performance and Reliability Monitor has a Resource Overview pane that displays the real-time usage of CPU, Disk, Network, and Memory on the local computer. This is better than the Task Manager to show real-time data. Table 3.1 describes the information shown in the Resource View detail screens.

**Table 3.1** Resource View Details

Label	Description
CPU	CPU displays the total percentage of CPU capacity currently in use by the local system. The capacity currently in use is displayed in green and displays the CPU Maximum Frequency in blue.
Image	The application that the local system is using CPU resources.
PID	The process ID of the application instance.
Description	The name of the application.
Threads	The number of threads that are currently active from the application instance.
CPU	The CPU cycles that are currently active from the application instance.
Average CPU	The average CPU load over the last 60 seconds resulting from the application instance, expressed as a percentage of the total capacity of the CPU.
Disk	Disk displays the total current Input/output in green and displays the highest active time percentage in blue.
Image	The application that is using disk resources on the local system.
PID	The process ID of the application instance.
File	The files that is being read and/or written by the application instance.
Read	The current speed (in Bytes/minute) at which the data is being read from the file by the application.
Write	The current speed (in Bytes/minute) at which data is being written to the file by the application.
IO Priority	The priority of the Input/output task for the application.
Response Time	The response time in milliseconds for the disk activity.
Network	Network displays the current total network traffic (in Kbps) in green and displays the percentage of network capacity in use in blue.
Image	The current application that is using network resources.

**Continued**

**Table 3.1 Continued.** Resource View Details

Label	Description
PID	The process ID of the application instance.
Address	The network address with which the local computer is exchanging information. This may be expressed as a NETBIOS name, as an IP Address or as a fully qualified domain name (FQDN).
Send	The amount of data (in Bytes/min) that the application instance is currently sending from the local computer to the address mentioned above.
Receive	The amount of data (in Bytes/min) that the application instance is currently receiving from the address mention above.
Total	The total bandwidth (in Bytes/min) that is currently being sent and received by the application instance mentioned above.
Memory	Memory displays the current hard faults per second in green and displays the percentage of physical memory currently in use in blue.
Image	The application that is using the memory resources.
PID	The process ID of the application instance.
Hard Faults/minute	The number of hard faults per minute that are currently resulting from the application instance. A hard fault (also known as a page fault) occurs when the page of the referenced memory address is no longer in physical memory and has been swapped out or is available from a backing file on disk. This is not an error—but, a high number of hard faults may explain the slow response time of an application if it must continually read data back from disk rather than from physical memory.
Working Set (KB)	The number of kilobytes that are currently residing in memory for the application instance.
Shareable (KB)	The number of kilobytes of the application instance working set that may be available for other applications to use.
Private (KB)	The number of kilobytes of the application instance working set that is dedicated to the application process.



### TEST DAY TIP

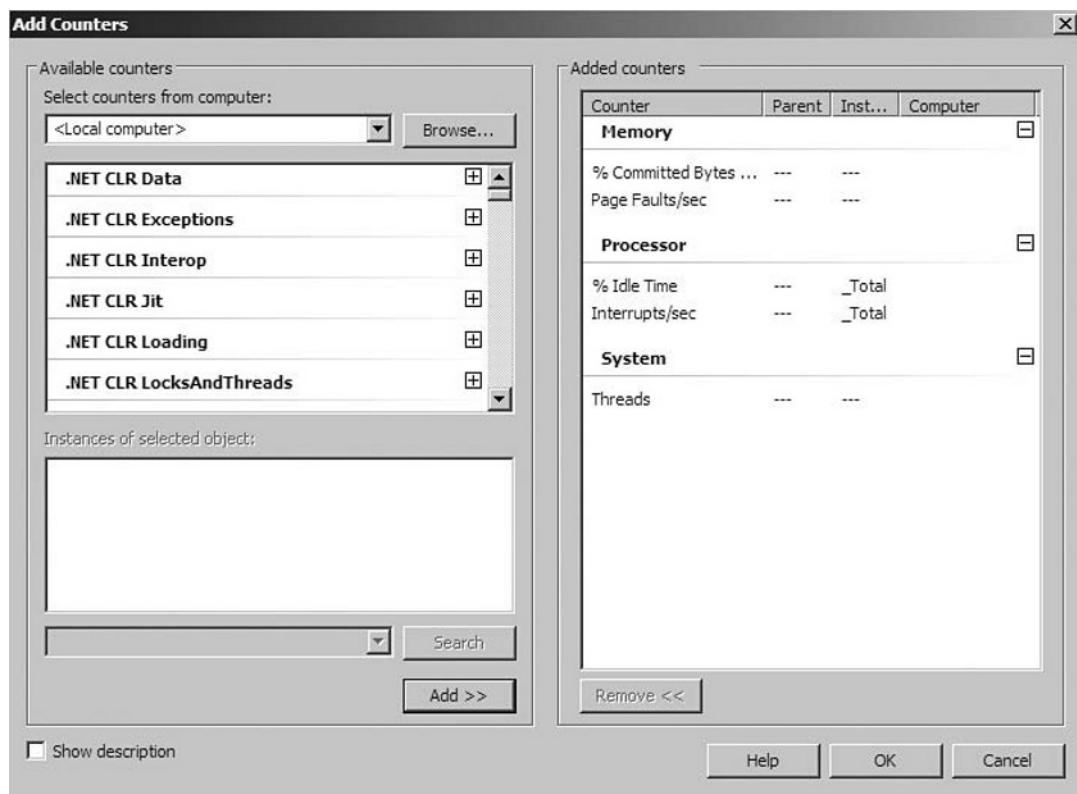
On the day of the exam, it is a good practice to go over terms and definitions. The previous table is a great example. Be sure to look over the definitions and make sure you understand the meanings and use. A good once-over before entering the testing center will increase your chances of passing the examination.

## EXERCISE 3.8

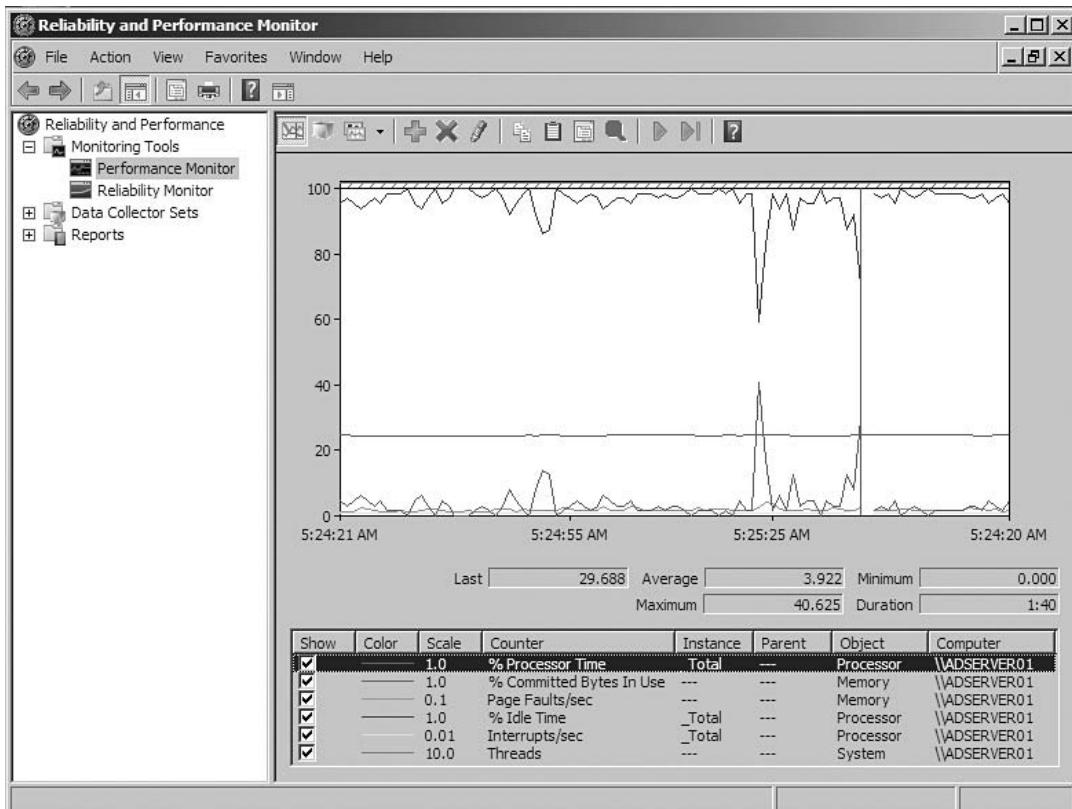
### MONITORING SYSTEM ACTIVITY USING PERFORMANCE AND RELIABILITY MONITOR

In this exercise, we are going to use the Performance and Reliability Monitor to add specific performance counters to the display, observe the data in real time, and learn how to pause the monitor to display and examine current system status.

1. Click **Start | Administrative Tools | Reliability and Performance Monitor**.
2. In left pane, expand **Monitoring Tools** then click **Performance Monitor**.
3. In the menu bar above the Performance Monitor graph display, click the **Add button (+)**. The **Add Counters** dialog box opens.
4. In the **Available Counters** section, select the following counters, and click **Add** to view in the Performance Monitor Display. See Figure 3.32 for a screenshot of the added counters.
  1. Memory: % Committed Bytes In Use
  2. Memory: Page Faults/sec
  3. Processor: % Idle Time
  4. Processor: Interrupts/sec
  5. System: Threads

**Figure 3.32** Add Counters

5. When you are finished adding the counters, click **OK**.
6. Observe the data in the line chart. Click the **Pause** button on the toolbar to freeze the display. See **Figure 3.33** for an example.

**Figure 3.33 Reliability and Performance Monitor**

7. Click **File** then **Exit** to close the Reliability and Performance Monitor.

## Optimization

Through trending and baseline analysis along with good performance monitoring, we are able to add resources intelligently to our servers—increasing the performance and efficiency of our server farm. Through optimization, we tune settings and parameters that can result in improved performance of a Microsoft Windows Server 2008 installation. The most effective tuning changes consider the hardware, the workload, and the performance goals the administrator is trying to reach. Tuning sometimes involves changing the registry settings; it is very important to backup your registry before making any changes.

Good optimization begins with the server hardware design—you must have the right hardware to satisfy expected server performance. Hardware bottlenecks cannot

be fixed by software optimization tuning. Table 3.2 lays out some server hardware recommendations that should be followed on any server design.

**Table 3.2** Server Hardware Recommendations

Component	Recommendation
Processors	Whenever possible, choose 64-bit processors over 32-bit processors—the increase in cost is worth the significant performance. Research data has shown that two CPUs are not as fast as one CPU that is twice as fast. Because it is not always possible to get a CPU that is twice as fast, doubling the number of CPUs is preferred, but it does not guarantee twice the performance. Memory and I/O performance need to be scaled to the processor speed or changing to a faster processor will not be beneficial. Do not compare CPU frequencies across manufacturers and generations; the comparison can be a misleading indicator of speed.
Cache	Larger L2 and L3 processor cache will improve the performance of a server. The larger caches generally provide better performance and often play a bigger role than raw CPU speed.
Memory	Memory is often the most overlooked component when sizing a server—memory needs to be sized according to the applications that are installed on the server. Windows Server 2008 will use hard drive space in a process called paging when physical memory has been exhausted. This causes a performance issue since hard drive access is a lot slower than physical memory access. Excessive paging degrades overall system performance. You can optimize the paging file by placing the operating system and paging file on different physical disks. Also, place the pagefile on a non-fault tolerant drive. If it is placed on a volume that is using RAID—the RAID controller performance will be degraded. Use multiple disks in a RAID 0 stripe set for the optimum paging file performance. Don't place pagefiles on different partitions on the same physical disk.
Bus	To avoid bus speed limitations, use either PCI-X or PCIe x8 and higher slots for Gigabit Ethernet adapters.

When designing the server hardware, you should also take into consideration networking and storage adaptors. The choice of adapters can significantly influence the performance of a server. Table 3.3 lists the recommended settings for choosing networking and storage adapters in a high performance Windows 2008 Server environment. By following these recommendations, you will keep these adaptors from being the bottleneck and causing performance issues.

**Table 3.3** Network and Storage Adapter Recommendations

Recommendation	Description
WHQL Certified	Make sure that all adapters have passed the Windows Hardware Quality Labs (WHQL) certification test suite.
64-Bit Capability	Adapters that are 64-Bit capable can perform direct memory access (DMA) operations to and from physical memory locations above 4GB. If the driver does not support DMA access above 4GB, the system will run degraded. Make sure you are using the most current driver available from the card manufacturer.
Copper and Fiber Adapters	Traditional copper adapters generally have the same performance as fiber adapters, and both copper and fiber are available on some Fiber Channel adapters. Certain environments are better suited to copper adapters—and some are better suited for fiber adapters. Fiber adapters are more common and offer the best performance overall.
Dual or Quad Port Adapters	With servers becoming smaller, multi-port adapters help save valuable PCI slots. Some SCSI adapters now have 2 and 4 ports to accommodate more disks and help break the SCSI limit barrier. Fiber Channel disks generally have no limits to the number of disks connected to an adapter unless they are hidden behind a SCSI interface (iSCSI). Serial Attached SCSI (SAS) and

Continued

**Table 3.3 Continued.** Network and Storage Adapter Recommendations

Recommendation	Description
Serial ATA (SATA) Adapters	Serial ATA (SATA) adapters also have a limited number of connections due to the serial nature of the protocols, but an increase in the number of attached disks is possible through switches.
Network Adapters	Network adapters have this feature for load-balancing or failover scenarios. Using two single-port network adapters usually yields better performance than using a single dual-port network adapter for the same workload.
PCI Bus Limitations	PCI bus limitation can be a major factor in limiting performance for multi-port adapters. Therefore, it is important to consider placing them in a high performing PCI slot like PCI-X or PCIe x8.
Interrupt Moderation	Some adaptors can do processing and offload activity from the CPU processor. Moderating interrupts can often result in a reduction in CPU load on the host but, unless interrupt moderation is performed intelligently, the CPU savings might cause increases in latency.
Offload Capability	Offload capable adapters offer CPU savings that translates into improved performance.

When considering server hardware, one of the other performance factors that needs to be taken into consideration is the storage subsystem. Decisions about how to design or configure storage software and hardware almost always consider performance. Performance is always sacrificed or enhanced as the result of trade-offs with other factors such as cost, reliability, availability, or ease of use. Table 3.4 analyzes the difference in RAID types and factors to consider for implementation. Each RAID level involves a trade-off between the following factors:

- Cost
- Performance
- Availability
- Reliability

**Table 3.4** Hardware RAID Levels

Option	Description
RAID 5	RAID 5 presents a logical disk composed of multiple physical disks with data striped across the disks in sequential blocks called stripe units. Parity information is distributed across all disks in the RAID. Read requests have the same performance of RAID 0—data writes are much slower than RAID 0 because each parity block that corresponds to the modified data block requires at least three additional disk requests. Thus, bandwidth is reduced by 75%. One disk can fail in RAID 5 configurations and still operate at a degraded level. RAID 5 is less expensive than RAID 1 (disk mirroring).
RAID 6	RAID 6 is the same as RAID 5; except you can lose two drives and the system will continue to work—though in a degraded state.
RAID 0	RAID 0 is data that is spread over multiple disks with no parity—so RAID 0 does not offer any type of redundancy. It presents a logical disk that stripes disk accesses over a set of physical disks. This type of RAID is the least expensive because all space is capable of storing data with no overhead for parity. For most workloads, a striped data layout provides better performance than other RAID levels if the strip unit is appropriately selected based on server workload and storage hardware characteristics.
RAID 1	RAID 1 is data mirroring. Although RAID 1 has the fastest recovery time because the disk are identical and can failover quickly—RAID 1 has the worse bandwidth and latency for write operations as compared to RAID 0. This is because data needs to be written

**Continued**

**Table 3.4 Continued.** Hardware RAID Levels

Option	Description
RAID 0+1	<p>to two or more physical disks. Sometimes RAID 1 can provide faster read operations than RAID 0 because it can read the disk that is least busy. RAID 1 is the most expensive RAID level because you need to have at least two disks for each copy.</p> <p>The combination of striping and mirroring provides the performance benefits of RAID 0 and the redundancy benefits of RAID 1. This RAID level is also known as RAID 1+0 and RAID 10.</p>

Microsoft does offer a software solution for Microsoft Windows Server 2008 Enterprise Edition and Windows Server 2008 Datacenter Edition to optimize performance and resources—this tool is called Microsoft Windows System Resource Manager (WSRM). WSRM is not installed by default and needs to be added to the base operating systems through the Windows Server 2008 Server Manager. WSRM provides resource management and enables the allocation of resources, including processor and memory resources, among multiple applications based on priorities set by the administrator. WSRM enables a system administrator to do the following:

- Set CPU and memory allocation policies on applications.
- Manage CPU utilization (percent CPU in use).
- Limit the process working set size (physical resident pages in use).
- Manage committed memory (pagefile usage).
- Apply policies to users or groups on a Terminal Services application server.
- Apply policies on date/time schedule.
- Generate, store, view, and export resource utilization accounting records from management, service level agreements (SLA) tracking, and charge back purposes.

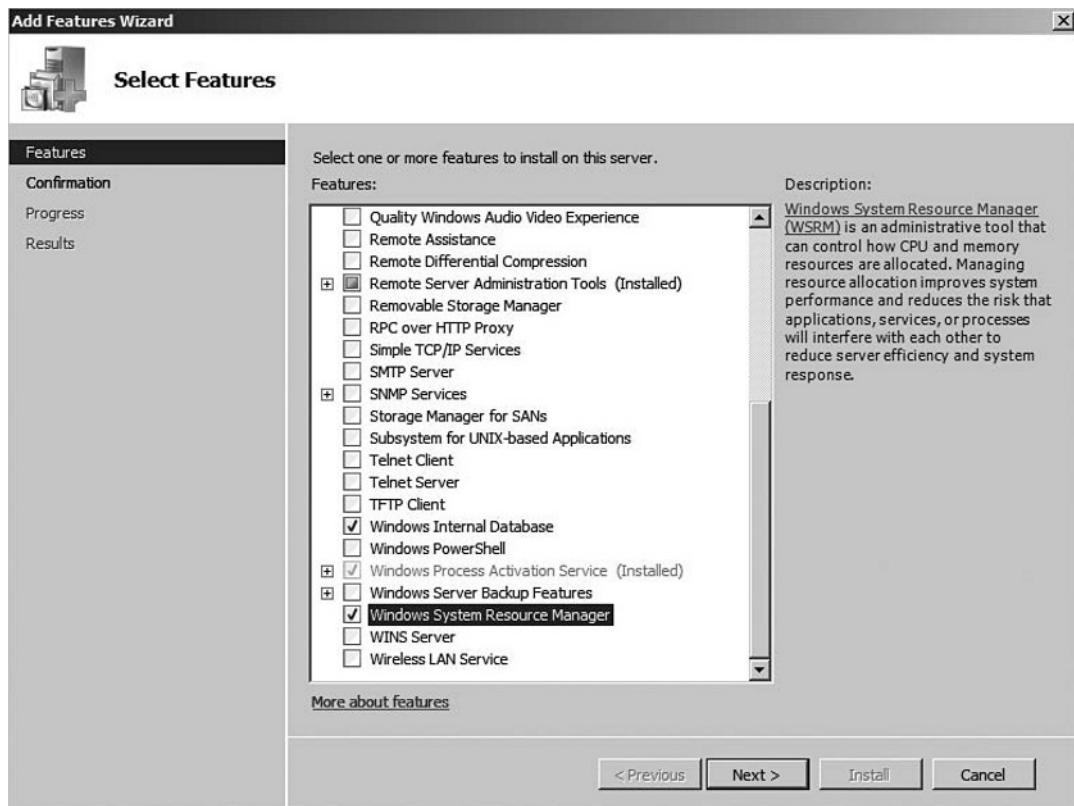
## EXERCISE 3.9

### ENABLING MICROSOFT WINDOWS SYSTEM RESOURCE MANAGER AND CREATING A PROCESS MATCHING CRITERIA

In this exercise, we are going to install the Microsoft Windows System Resource Manager (WSRM) and configure a Process Matching Criteria. To do this exercise you will need to be working with Microsoft Windows Server 2008 Enterprise Edition.

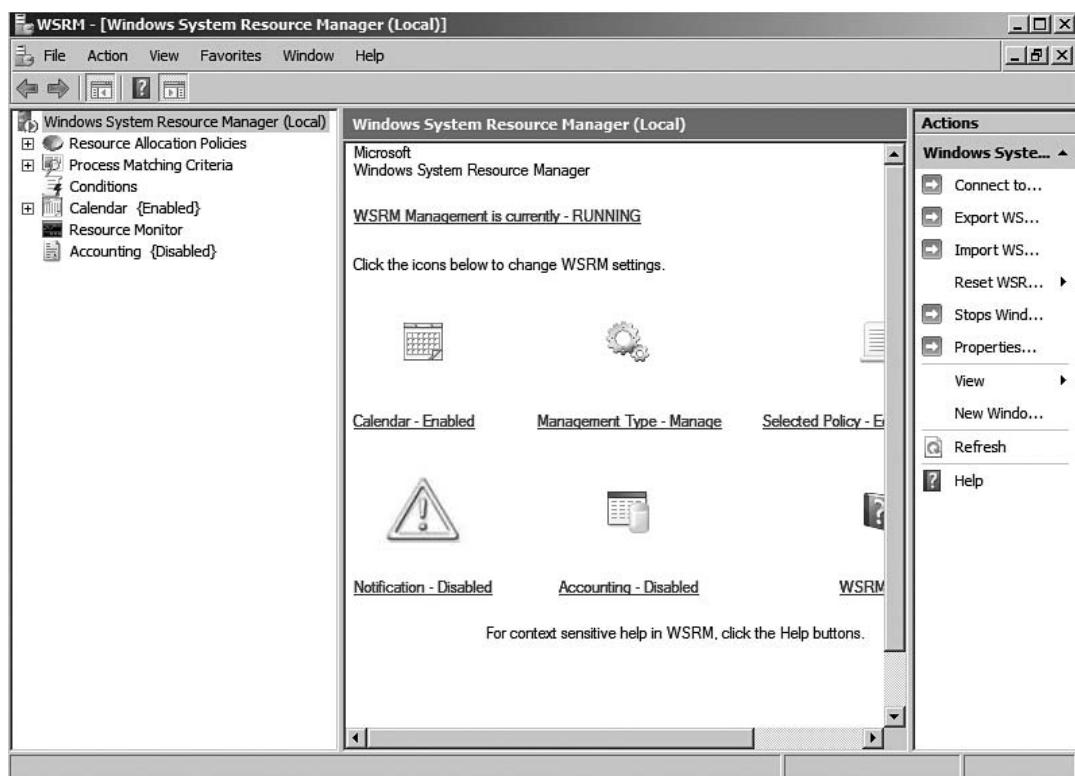
1. Click **Start** and open **Server Manager**.
2. Click **Features** in the left pane tree and then click **Add Features** in the right pane.
3. In the **Add Features Wizard**, select **Windows System Resource Manager**. When prompted to **Add Required Features** click **Add Required Features**. See Figure 3.34.

**Figure 3.34** Add Features Wizard



4. Click **Next**.
5. In the **Confirm Installation Selections**, click **Install**.
6. When the **Installation Results** window come up, verify that all installations where successful. Click **Close** to finish the installation.
7. Click **File** then **Exit** to close the **Server Manager**.
8. Click **Start | Administrative Tools | Windows System Resource Manager**. When prompted to **Connect to computer** choose **This computer** and click **Connect**. The Windows System Resource Manager Windows should look like Figure 3.35.

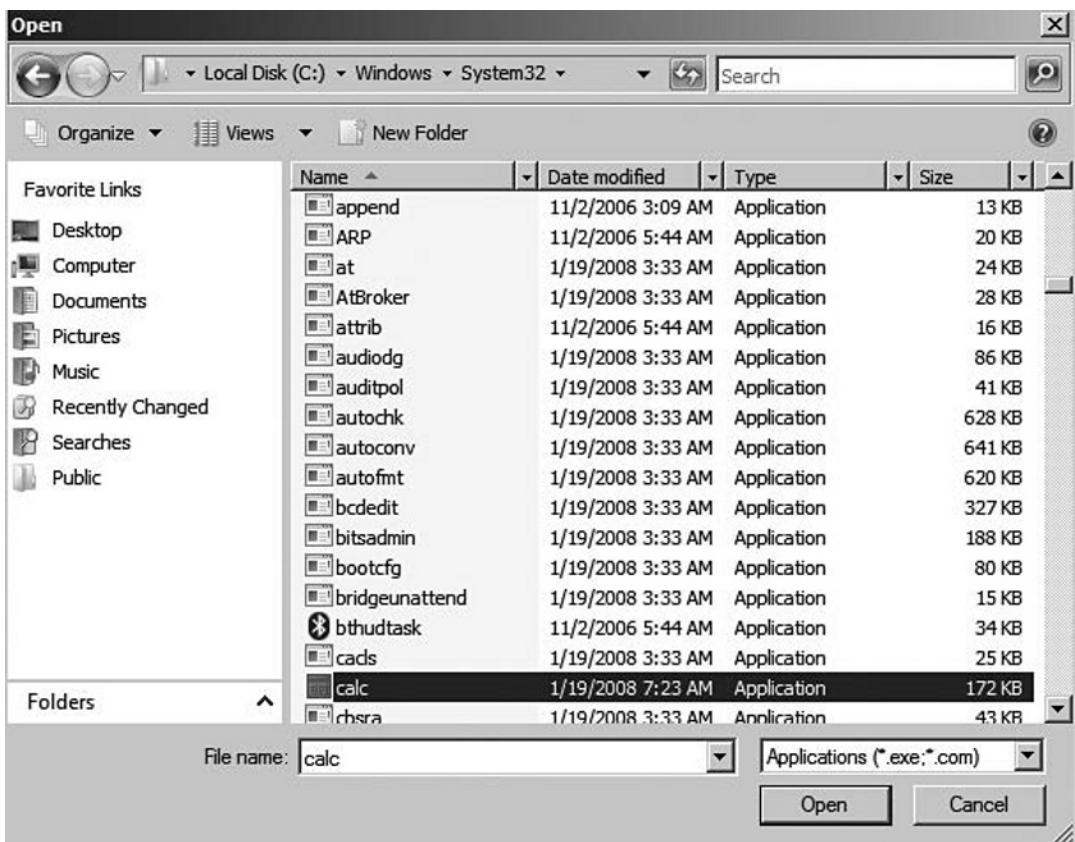
**Figure 3.35** Windows System Resource Manager



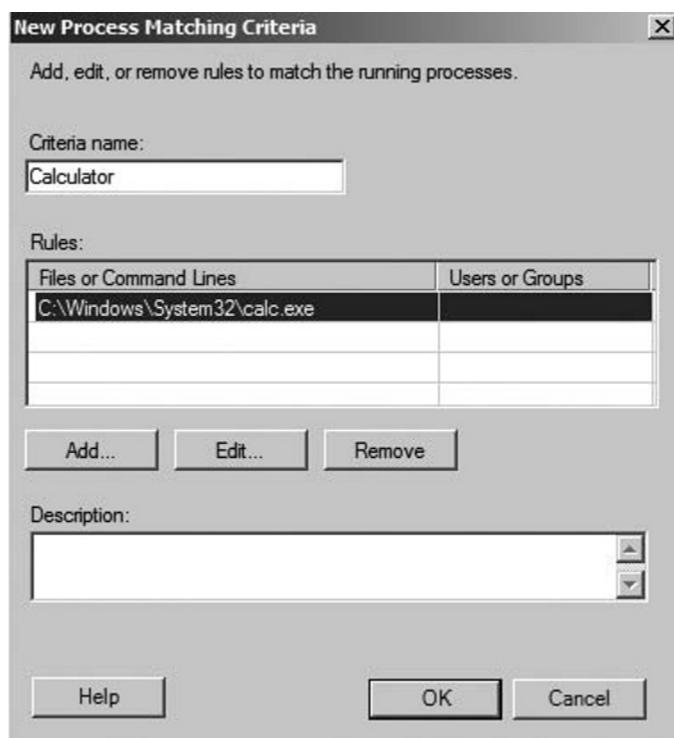
9. In the left pane, right-click **Process Matching Criteria** and select **New Process Matching Criteria...**
10. In the **New Process Matching Criteria**, enter **Calculator** as the **Criteria name**.

11. Click the **Add** button.
12. In the **Add Rule** windows, click the drop-down menu and select **Application**.
13. Click **Select**. The **Open** window comes up. Drill down to the **calc.exe** (Calculator) and select **Open**. See Figure 3.36 for an example.

**Figure 3.36 Open**



14. The **Add Rule** window now shows the Calculator program. Click **OK** to continue.
15. Then a **New Process Matching Criteria** window now shows the **Calculator** program. See Figure 3.37. Click **OK** to finish creating the **New Process Matching Criteria**.

**Figure 3.37** New Process Matching Criteria

16. Click File | Exit to close the Windows System Resource Manager.

---

## Event and Service Management

Microsoft has improved the service recovery in Microsoft Windows Server 2008. The ability still exists to set a process to recover from a failed service or service event. This can be restarting the service a certain number of times or running a script or executable file. More services can be restarted or recovered without a reboot—which saves the administrator a lot of unplanned reboots. For instance, it is now possible to restart the Active Directory with a reboot.

Another really big improvement is with the way Microsoft Windows Server 2008 can handle events with the Event Viewer. With Microsoft Windows Server 2008, you can easily select any event and create an action to recover the error. For instance, if a print job failed—you could have Microsoft Windows Server 2008 run a script to purge the print queue. The possibilities are endless with the actions you can create from events in the Event Viewer.

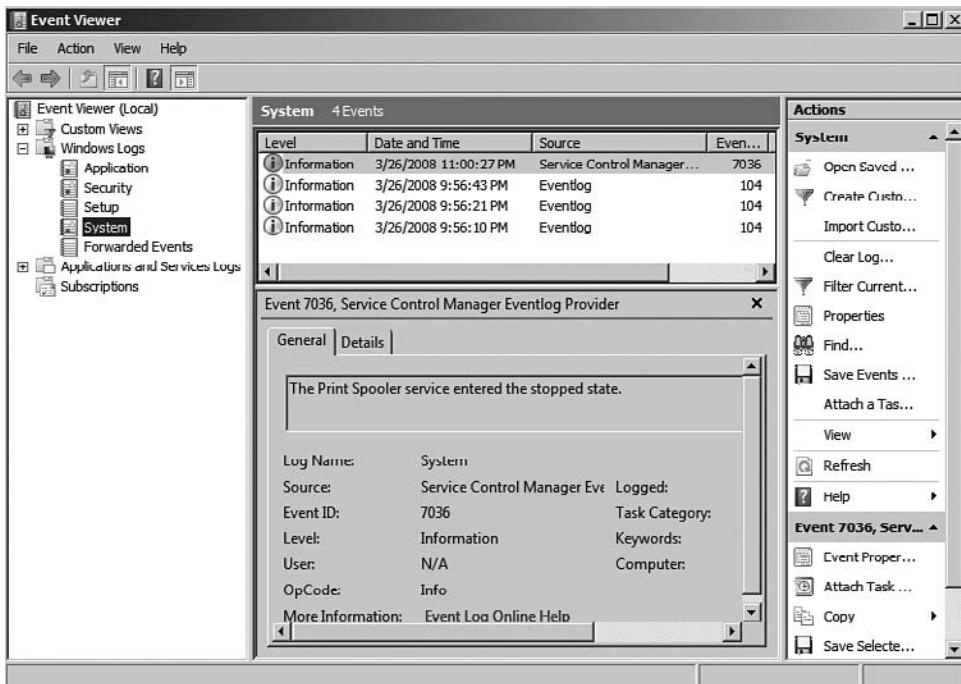
## EXERCISE 3.10

### CREATE AN ACTION BASED ON AN EVENT VIEWER EVENT

In this exercise, we are going to create an action in the Event Viewer that will restart the Print Spooler if it would stop.

1. Click **Start** then **Run**.
2. In the **Run** command box, type **Net Stop Spooler**. This will create an event in the System Log for us to work from in this exercise.
3. Click **Start | Administrative Tools | Event Viewer**.
4. In the left pane, expand **Windows Logs** then select **System**. See Figure 3.38.

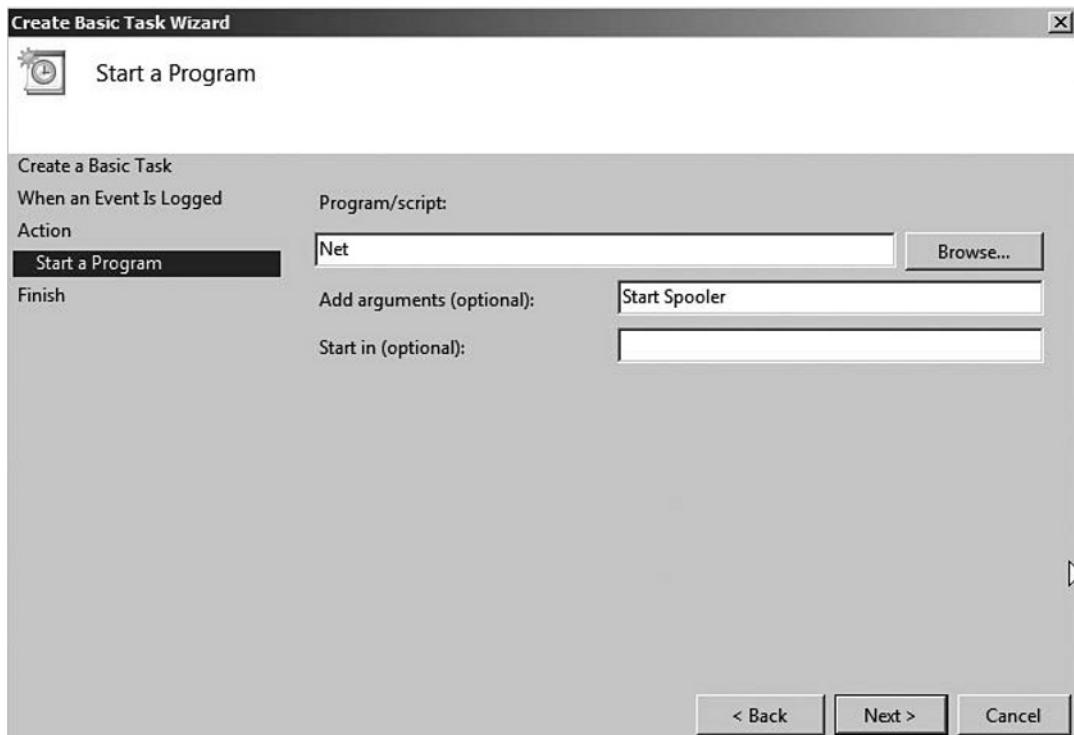
**Figure 3.38** Event Viewer



5. Select the **Service Control Manager** event and right-click and select **Attach Task To This Event...**
6. In the **Create Basic Task Wizard**, rename the **Restart Print Spooler**. Click **Next**.

7. Click **Next** at the **When a Specific Event Is Logged** screen.
8. In the **Action** screen choose **Start a program** and click **Next**.
9. At the **Start a Program** windows, enter **Net** for the **Program/script** and **Start Spooler** for the **Add arguments (optional)**. See Figure 3.39. Click **Next**.

**Figure 3.39** Create Basic Task Wizard



10. At the **Summary** window, click **Finish**.
11. Click **OK** at the **Event Viewer** dialog box.
12. Click **Start**, and then **Run**. Type **Net Start Spooler** and press **Enter**.
13. Click **Start**, and then **Run**. Type **Net Stop Spooler** and press **Enter**. Notice that when the spooler stops, another window comes up and starts the spooler again. The task you created is working properly.
14. Click **File**, and then **Exit** in the **Event Viewer**.

## Trending and Baseline Analysis

When you first install a server, you should run a baseline analysis against it during normal operation—I would like to stress *during normal operation*. A baseline analysis taken when there is no load on the server will not help when you actually need the data. Baseline analysis helps you when the server begins to run slow and you want to compare the performance metrics to when the server was first installed. This takes user perception out of the picture and allows for real data to back up claims that the server is running slow.

Whenever you are doing baseline and trending, it is important to take into consideration the key components in your system. You should consider the server role and workload to determine which hardware components are likely to restrict the performance of the server. If we were baselining and trending a SQL Server, there would be differences in the components monitored compared to an IIS Server.

Common performance metrics that are commonly monitored include:

- Cache
- Memory
- Objects
- Paging File
- Physical Disk
- Processes
- Processor
- Server Jobs
- System Processes
- Threads

You should familiarize yourself with basic performance measurement objects (including the ones listed above) and counters to monitor the main hardware components.

When monitoring the servers, we want to use logging and collect data over a period of time to give us a real analysis of the situation. This data should be stored so it can be compared to other collections over the history of the server. Doing this will help us plan for future business requirements and may possibly lead to reducing the number of servers in operation after measuring performance. It is important to consider performance analysis alongside business plans—this way the servers are being utilized to their full potential.

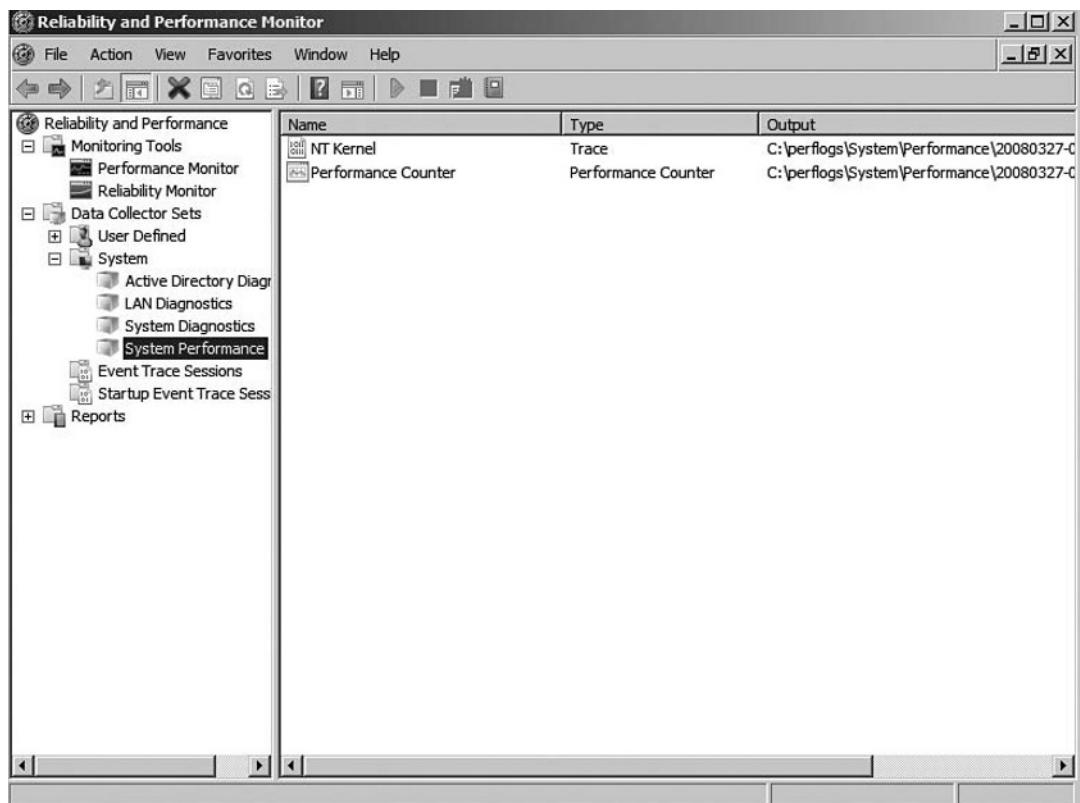
## EXERCISE 3.11

### COLLECT LOGGING DATA IN THE RELIABILITY AND PERFORMANCE MONITOR

Microsoft has provided some Data Collector Sets that will do a good job performing a server baseline analysis. In this exercise, we are going to use one of these Data Collector Sets to perform a baseline analysis over 5 minutes. Normally you would do the analysis over a 24 hour period or maybe even longer.

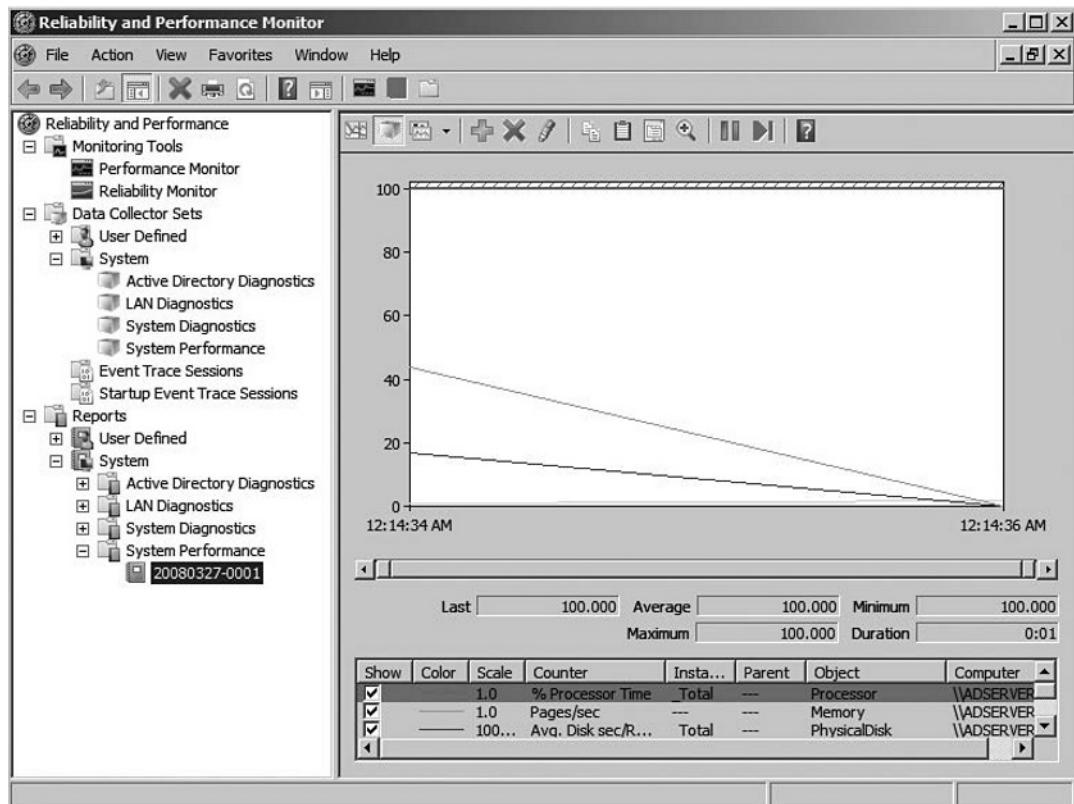
1. Click Start | Administrative Tools | Reliability and Performance Monitor.
2. In the left pane, expand Data Collector Sets and then expand System.
3. Select System Performance. See Figure 3.40.

Figure 3.40 Reliability and Performance Monitor



4. Right-click **System Performance** and click **Start**. Notice the play symbol on **System Performance**—this means that it is performing data collection. Wait 5 minutes.
5. Right-click **System Performance** and click **Stop** to end the data collection process.
6. Notice after you stop the Data Collector—there is a folder called **Reports** at the bottom of the left pane tree. Expand **Reports**, and then **System**. Now expand **System Performance**.
7. Click on the report under **System Performance**. The right pane shows information from the Data Collection. See Figure 3.41. This report can be saved and used later to compare to recent data.

**Figure 3.41 Reliability and Performance Monitor**



8. Click File, and then Exit to close the Reliability and Performance Monitor.

## Summary of Exam Objectives

Microsoft Windows Server 2008 makes Windows Server Update Services available for free to maintain patches and operating system updates on Microsoft supported operating systems which include the following: Microsoft Windows Server 2008, Microsoft Windows Vista, Microsoft Windows Server 2003, Microsoft Windows XP Professional, and Microsoft Windows 2000 Service Pack 4 (any edition). WSUS is very granular in its design—allowing for customizing of the installation to suit the network infrastructure. The current version of WSUS is 3.0 Service Pack 1. When deploying WSUS 3.0 Service Pack 1 on Microsoft Windows Server 2008, you need the following software installed: Microsoft Internet Information Services (IIS) 7.0 with Windows Authentication, ASP.NET, IIS Version 6 Management Compatibility, IIS Version 6 Metabase Compatibility, Microsoft Report Viewer Redistributable 2005 and Microsoft SQL Server Service Pack 1.

Operating system patch management can be done in two ways. The first method would be to use Windows Update. Windows Update goes out to the Microsoft Web site and downloads the necessary updates. Microsoft Windows Server 2008 does not have Windows Update enabled by default. The second method is to use WSUS on the network. WSUS is the best choice for better administration of the clients—you have the opportunity to test patches before making them available to the production network. WSUS can also patch Microsoft application products.

WSUS can be installed in two different modes. Autonomous Mode: An upstream WSUS server shares updates with its downstream server or servers during synchronization, but no update approval status or computer group information. Downstream WSUS servers must be administered separately. Autonomous server can also synchronize updates for a set of languages that is a subset of the set synchronized by their upstream server. Replica Mode: An upstream WSUS server shares updates, approval status and computer groups with its downstream server or servers.

Microsoft WSUS 3.0 Service Pack 1 has added a new feature that allows you to manage the WSUS server from a remote workstation via a Microsoft Management Console (MMC). The WSUS MMC installation is supported on Microsoft Windows Server 2008, Microsoft Windows Vista, Microsoft Windows Server 2003 Service Pack 1, and Microsoft Windows XP Service Pack 2. You also need to have the following installed: Microsoft .Net Framework Version 2 Redistributable Package, Microsoft Management Console 3.0 for Windows Server 2003, and Microsoft Report Viewer Redistributable 2005.

WSUS can push updates to the following operating systems: Microsoft Windows Vista, Microsoft Windows Server 2008, Microsoft Windows Server 2003, Microsoft

Windows XP Professional and any version of Microsoft Windows 2000 Service Pack 4. The easiest way to push the settings to the clients for WSUS is Group Policy Objects in Active Directory. If your network is a workgroup, you can change the Local Group Policy Object to point at a WSUS server.

System monitoring is one of the most often overlooked responsibilities of a network administrator. The key reasons to monitor your system include the following: health of the IT Infrastructure, Service Level Agreement Monitoring, planning for future requirements, and identifying issues.

New features of the Microsoft Reliability and Performance Monitor include: Data Collector Sets, Wizards and Templates for creating logs, Resource Overview, Reliability Monitor, Unified property configuration for all data collection, and user-friendly diagnostic reports.

When performing server optimization, the most important task is to choose the appropriated hardware to match the server role in the network infrastructure. The hardware to pay close attention to includes the processors, processor cache, memory, and the server I/O bus. When planning a server installation, pay particular attention to the storage subsystem—the RAID levels can significantly weigh in on the performance of the server. RAID levels include: RAID 5, RAID 6, RAID 0, RAID 1, and RAID 0+1.

When you first install a server, you should run a baseline analysis against it during normal operation. Baseline analysis helps you when the server begins to run slow and you want to compare the performance metrics to when the server was first installed. This takes user perception out of the picture and allows for real data to back up claims that the server is running slow.

### EXAM WARNING

For this exam, it is not only important to understand performance counters and optimal hardware choices, but you need to be able to interpret Microsoft Reliability and Performance Monitor data. Some of this information is beyond the scope of this book—a book on interpreting performance monitor data alone could be written. I would recommend that if you are not very familiar with hardware and how it affects performance that you visit Microsoft TechNet and read some of the available whitepapers on this topic.

# Exam Objectives Fast Track

## Patch Management

- Microsoft Windows Server Update Services 3.0 Service Pack 1 (WSUS) is the patch management system from Microsoft that is freely available.
- Operating system patch management can be performed with Windows Update or WSUS.
- Microsoft Internet Information Services (IIS) 7.0 must be installed where the WSUS server resides.
- WSUS installation requirements are IIS 7.0, Microsoft Report Viewer Redistributable 2005, and Microsoft SQL 2005 Service Pack 1.
- WSUS requires that the system partition and the partition where WSUS is located be formatted with NTFS.
- WSUS can be installed in Autonomous Mode or Replica Mode.
- WSUS is managed through a Microsoft Management Console (MMC) and can be managed from a remote client.
- Application patching on Microsoft products can be done with WSUS.

## Monitoring for Performance

- Microsoft Reliability and Performance Monitor is used to monitor a Microsoft Windows Server 2008.
- Data Collector Sets can be reused and exported to other Microsoft Windows Server 2008 servers.
- Microsoft Reliability and Performance Monitor calculates a System Stability Index that reflects the state of the server.
- Processors, memory, cache and I/O bus are the most important components to monitor for server optimization.
- Each RAID level involves a trade-off between cost, performance, availability, and reliability.
- Microsoft Windows System Resource Manager (WSRM) is available with Microsoft Windows Server 2008 Enterprise Edition.
- WSRM allows you to optimize performance and resources through Process Matching Criteria and policies.

# Exam Objectives

## Frequently Asked Questions

**Q:** This chapter has a lot of new acronyms that I have never heard before. Will the exam use acronyms and what is the best way to learn them?

**A:** The exam will definitely use acronyms to try and throw you off on a question. The best way to learn acronyms is to use index cards to make flash cards.

**Q:** My employer has not installed or migrated to Windows Server 2008 yet. Should I get hands-on experience before sitting this exam?

**A:** Yes! The best advice for any Microsoft exam is to actually sit down and work with the product. Go out and download the free copy of Microsoft Virtual PC 2007 and register for a 180 day trial of Windows Server 2008 Enterprise Edition. With Microsoft Virtual PC 2007, you can use multiple virtual machines to build virtual networks. This way you can setup just about any scenario in a test environment.

**Q:** In the section on performance and optimizing, there is a lot of information on monitors and hardware designs. Will this information be tested? It does not seem like it would be Microsoft specific and should not be included on the exam.

**A:** Questions regarding performance are going to include hardware answers. Remember this exam is going to test your understanding on how to optimize a server. To do this, hardware design is important. Make sure you understand RAID levels and hardware characteristics mentioned in this chapter.

**Q:** What is the information in this chapter that causes students the most problems on the exam?

**A:** Definitely the monitoring and optimizing subjects. Students tend to ignore hardware characteristics and important counters to monitor a server's performance. Remember that when you optimize a server, it is very important to consider its role in the network infrastructure. For example: A Microsoft 2005 SQL Server is going to need a very fast storage subsystem and plenty of memory and processor performance. It may be beneficial to visit Microsoft TechNet (<http://technet.microsoft.com>) and do some research on performance monitoring and optimization.

**Q:** There is a lot of data presented in tables in this chapter. Is it important to memorize this data?

**A:** I would definitely memorize the RAID levels for this exam. Understanding the concepts of performance monitoring is more important than memorizing the information. Understand how each server component relates to the overall performance of the server.

**Q:** In this chapter, you mentioned that Microsoft Windows System Resource Manager (WSRM) is only available with Microsoft Windows Server 2008 Enterprise Edition. Will the exam cover Microsoft Windows Server 2008 Enterprise Edition?

**A:** Microsoft Windows Server 2008 Enterprise Edition is fair game on this exam. It is important to understand what WSRM does and how to manipulate settings and create Process Matching Criteria and policies.

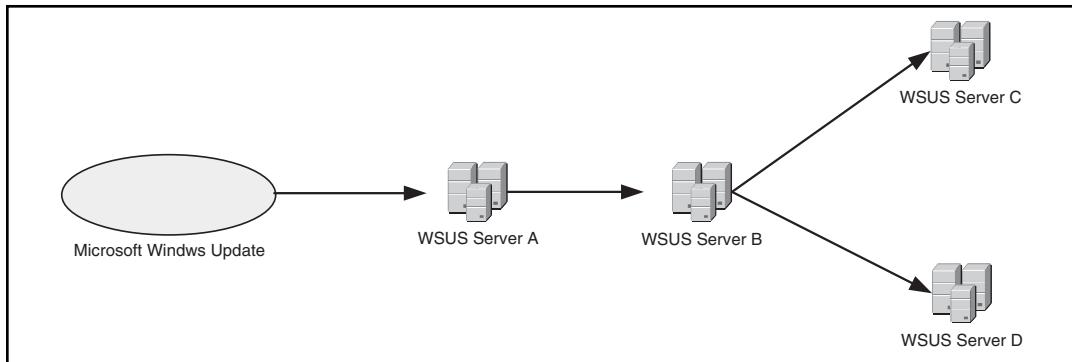
## Self Test

1. Microsoft makes a free server-based patch solution available to customers for Microsoft current operating systems. This free server software is:
  - A. Microsoft Update
  - B. Windows Update
  - C. Windows Server Update Service
  - D. Microsoft System Center Essentials 2007
2. There are two ways Microsoft makes available to update the Windows Server 2008 operating system. These two types of operating system patch management include:
  - A. Microsoft Windows Server Update Services
  - B. Windows Update
  - C. Microsoft Update
  - D. Internet Explorer 7.0
3. Your assistant Jim has just installed a new copy of Microsoft Windows Server 2008. You do not use Microsoft WSUS on your network. You instruct Jim to configure automatic updates through Windows Update on the newly installed server. Where could Jim configure this setting on the server?
  - A. Computer Management
  - B. Server Management
  - C. Internet Explorer 7.0 Options
  - D. Windows Update Control Panel
4. You wish to obtain the proper licensing for Microsoft Windows Server Update Service 3.0 SP1 for your network infrastructure. What are the proper licenses you must acquire to have a legal installation of WSUS?
  - A. Internet Information Service 7.0
  - B. Windows Server 2008
  - C. None
  - D. Windows Server 2003 Advanced Edition

5. When installing Microsoft Windows Server Update Services 3.0 SP1 on Windows Server 2008, we need to make sure that Internet Information Server 7.0 is configured with the proper components. Which of the following are components that are needed for a successful WSUS 3.0 SP1 installation?
  - A. IIS Version 7 Management Compatibility
  - B. ASP.NET
  - C. Windows Authentication
  - D. IIS Version 7 Metabase Compatibility
6. What Microsoft operating systems can support a Microsoft Windows Server Update Service 3.0 SP1 installation for the server part of the installation?
  - A. Microsoft Windows Server 2008
  - B. Microsoft Windows Server 2003
  - C. Microsoft Windows Server 2000 Advanced Edition
  - D. Microsoft Windows 2003 with Service Pack 1
7. You are installing the Microsoft Windows Server Update Service 3.0 SP1 on a Windows 2008 Server. The server has a system drive that is formatted with FAT32 and a second drive that is formatted with NTFS and is compressed. The installation fails repeatedly. What do you need to do to make the installation work properly?
  - A. Uncompress the NTFS partition then continue installation.
  - B. Convert the FAT32 drive to NTFS and uncompress the NTFS partition—continue installation.
  - C. Run Windows Update.
  - D. Resize the NTFS partition and continue the installation.
8. After installing Microsoft Windows Update Services 3.0 SP 1 on a Microsoft Windows 2008 Server you initiate the first synchronization. The WSUS directory grows in an excess of 20 GB. What would likely cause this to happen?
  - A. The WSUS directory is on a FAT32 partition.
  - B. WSUS is installed on a compressed drive.
  - C. All languages are selected in the configuration.
  - D. The WSUS server is in replica mode.

9. Consider the WSUS server hierarchy shown in Figure 3.42; which server would be considered the primary upstream server?

**Figure 3.42** WSUS Server Hierarchy



- A. WSUS Server A
  - B. WSUS Server B
  - C. WSUS Server C
  - D. WSUS Server D
10. An upstream WSUS server shares updates with its downstream server or servers during synchronization, but not update approval status or computer group information. Downstream servers must be administered independently from the upstream server. What mode would the upstream server be in this design?
- A. Replica Mode
  - B. Independent Mode
  - C. Autonomous Mode
  - D. Server Core Mode

## Self Test Quick Answer Key

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

This page intentionally left blank

# Chapter 4

## MCITP Exam 646

### Security and Policies

#### Exam objectives in this chapter:

- Remote Access Security
- Server Security
- Auditing

#### Exam objectives review:

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

# Introduction

Security is not a project. Security is not a task. Security is not something that you implement and walk away from. Security is, in fact, a way of life for IT organizations today. The tools and policies that we implement are what make up the security strategy which will guide the organization in their plans to provide for the “CIA Triad,” which stands for Confidentiality, Integrity, and Availability. The CIA triad is considered the generally accepted principals of information assurance. Achieving the CIA triad is relevant whether the data is in storage, processing, or transit, and whether threatened by intent or by error.

Microsoft for some time has been making security its main priority with the Microsoft Trustworthy Computing initiative. Starting with Microsoft Windows 2003 Server we were introduced to Network Access Quarantine Control. This feature enabled administrators to control remote access to a private network until the remote computer was validated by a script. The components necessary to deploy this solution included Microsoft Windows 2003 remote access servers, the Connection Manager Administration Kit, and Internet Authentication Service.

With Microsoft Windows 2008 Server, Windows Vista, and Windows XP Service Pack 3, Microsoft has introduced Network Access Protection (NAP). NAP can control virtual private network (VPN) connections better than Network Access Quarantine Control, but NAP can also enforce policy compliance through the following types of network access or communications:

- Internet Protocol security (IPsec) protected traffic
- IEEE 802.1x authenticated network connections
- Dynamic Host Configuration Protocol (DHCP) address configurations
- Remote access VPN connections

While new features such as NAP help to ensure that client security is up to company-mandated levels, we still need tools to protect the server itself. With Windows Server 2008, Microsoft has continued the usage of familiar tools such as the Encrypted File System (EFS), but also introduced new features such as BitLocker. At the same time, Microsoft has continued to develop their client-side firewall, now providing advanced functionality for granular management of communications.

In this chapter, we will discuss some of the technologies that are native to Microsoft Windows Server 2008, which will help you in your quest to achieve a higher level of confidentiality, integrity, and availability. Specifically, we will focus on

three key areas for security your environment. First, we will focus on protecting our internal assets while providing remote capabilities through the use of Remote Access. Next, we will focus on a new technology known as Network Access Protection, which uses health policies to determine the health status of a client. Finally, we will change our focus to auditing and reporting on security-related activities within our environment. Let's begin our discussion with Remote Access Security.

## Remote Access Security

Remote access solutions have been in demand for a number of years now. Since public access to the Internet had become available, employees were looking to utilize solutions to work from remote locations. Many companies allowed these employees to “telecommute” to work, but only in small numbers. However, as the cost of transit to corporate offices increased, the cost of high speed bandwidth decreased, and the focus of many businesses (and individuals) turned to becoming more “green,” more and more employees were taking advantage of this type of work atmosphere. However, as the same technologies that enabled “anywhere access” such as free Wi-Fi, cheaper broadband connectivity, and do-it-yourself home wireless became more widely adopted, would-be hackers were looking for new ways to exploit these new avenues and technologies.

One of the early solutions for secure remote access was direct-dial remote access, where end-users would use a legacy modem and an analog circuit to dial into a bank of corporate modems for access to the network. In this scenario, each user would use a traditional challenge/response type method (typically a username and password combination) to gain access to the network. Once connected, the users would be assigned an IP address and then be able to use corporate resources remotely. This solution was fairly secure, but very limiting due to the amount of bandwidth available. Over time, Virtual Private Networks (VPNs) became the norm. In a VPN scenario, and users would use a client application to perform the same challenge/response, however they would first establish a connection to the public Internet typically over DSL, cable, or other types of medium including dial-up to an Internet Service Provider (ISP). VPNs were (and still are) a great solution to provide remote access to the corporate line of business systems, but they were often gateways for viruses, worms, and overall malware to gain access to corporate networks.

Over time, new solutions for remote access became available:

- **Outlook Anywhere** Support for full Outlook access to Exchange. Allows for a user to take advantage of the feature-rich client without the need for a VPN, but data is still transmitted securely via HTTPS.

- **Office Communicator Remote Access** Support for corporate IM and presence, again encapsulated in HTTPS for security.
- **Terminal Services RemoteApp** Remote access via the Remote Desktop Protocol (RDP) to line-of-business applications by encapsulating the RDP session in HTTPS.

Even with all these great tools which allowed for remote access without a VPN, there is often still a need for a VPN connection to the corporate network in certain situations. On occasion, remote users may need to physically be present in the corporate office for a variety of reasons. Because of the work habits of “road warrior” users, as well as general telecommuters, Windows Server 2008 continues to offer remote access solutions, as well as new tools to protect corporate assets from the potential security risks associated with mobile computing.

In this section, we will take a look at a new role in Windows Server 2008, known as the Network Policy and Access Services Role (NPAS). For those of you familiar with the Internet Authentication Service (IAS) in Windows Server 2003, you will see that Microsoft has built upon that framework, and extended it for the next generation of remote access security. NPAS is ultimately a role that consists of a number of services:

- Network Policy Server (NPS)
- Routing and Remote Access Service (RRAS)
- Health Registration Authority (HRA)
- Host Credential Authorization Protocol (HCAP)

NPS is basically Microsoft’s version of a common solution known as Remote Authentication Dial-In User Service (RADIUS) server. RADIUS technologies allow you to control access via various solutions such as 802.1X and wireless access points, VPN servers, and legacy dial-up services. Routing and Remote access controls VPN connectivity via protocols such as Point-to-Point Tunneling Protocol (PPTP), Secure Socket Tunneling Protocol (SSTP), and Layer Two Tunneling Protocol (L2TP) with Internet Protocol security (IPsec).

HRA controls the distribution of health certificates to clients for use with Network Access Protection.

Likewise, HCAP integrates the Microsoft NAP solution with Cisco’s NAC solution. Obviously, there is a lot of information to absorb. First, let’s take a look at how NPAS is configured on a Windows Server 2008 system, and how we monitor and maintain NPAS in a Windows environment.

## New & Noteworthy...

### Cisco Network Access Control (NAC)

Similar to Microsoft, Cisco has been expanding their NAC solution for quite a while now. They have both a software and appliance solution (known as Clean Access). However, both companies formed the partnership simply because they knew that neither product could truly stand by itself. The Operating System needs the network, and the network needs the features and functions for security provided by the OS. To learn more about Cisco's NAC solution, visit [http://www.cisco.com/en/US/netsol/ns466/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html).

## Installing and Configuring NPAS

Many of the functions that you are used to using or working with from previous versions of the Windows Server operation system have been transformed into “roles” in Windows Server 2008. The Network Policies and Access Services Role is the same. As we mentioned NPAS is a role that has many services wrapped into one larger package. However, we do not have to install all of these roles at once. In our initial example, we will walk through the process of installing the Routing and Remote Access Server service. As you will see, the process is identical for each of the services. Similarly, you can return through the installation process and install other services even after the initial role is configured.

## Routing and Remote Access Service

As if Microsoft has not stacked enough services within the NPAS role, they have gone a layer deeper with the Routing and Remote Access Service (RRAS). Now turned into a role, the Routing and Remote Access Service portion of NPAS is actually two services in one. First, the routing function provides the ability to offer a fully-functional software-based router to direct traffic through both a local area network (LAN) or wide area network (WAN). RRAS supports industry standard routing protocols such as Routing Information Protocol (RIP) and Internet Group Management Protocol (IGMP). Microsoft introduced the concept of software

routing in earlier versions of the server operating system, and it has proven to be a cost-effective routing solution for many environments.

Likewise, the remote access portion of the RRAS service allows for a low-cost remote access solution. There are many companies who provide software and hardware remote access solutions, but Microsoft essentially gives it away with the OS. RRAS supports three different VPN protocols:

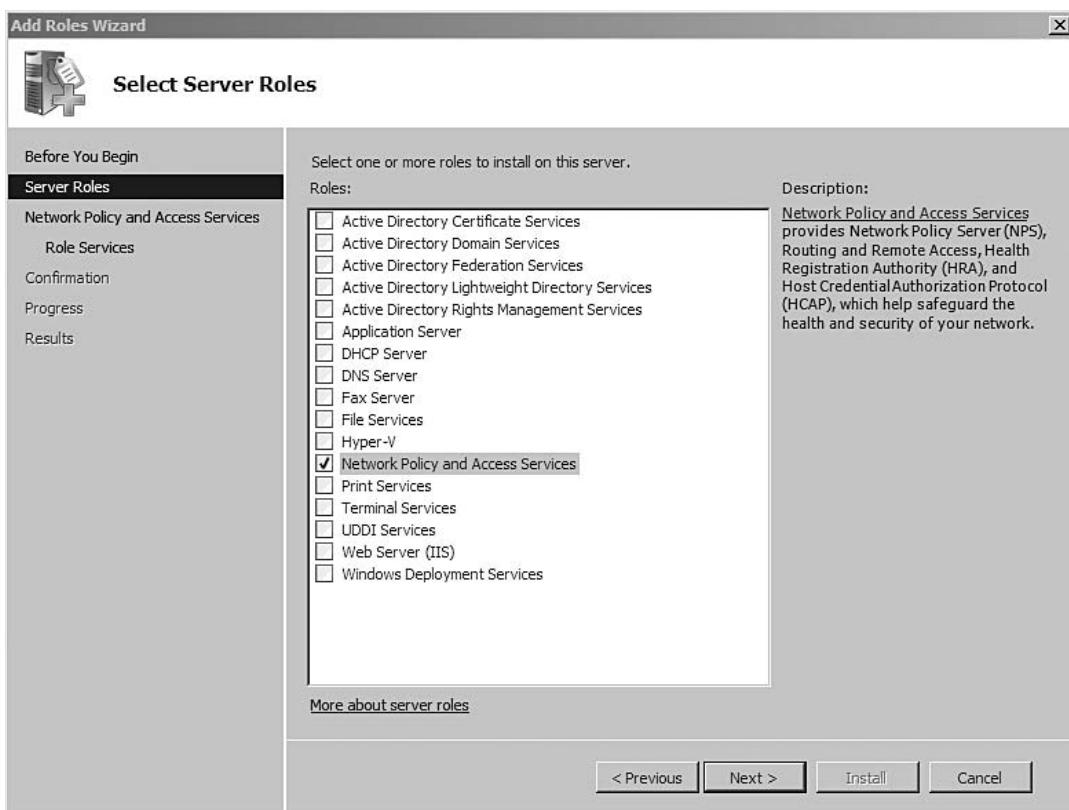
- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Tunneling Protocol (SSTP)
- Layer Two Tunneling Protocol (L2TP) with Internet Protocol security (IPsec)

We will step through the setup and configuration of these protocols after we discuss the initial installation process.

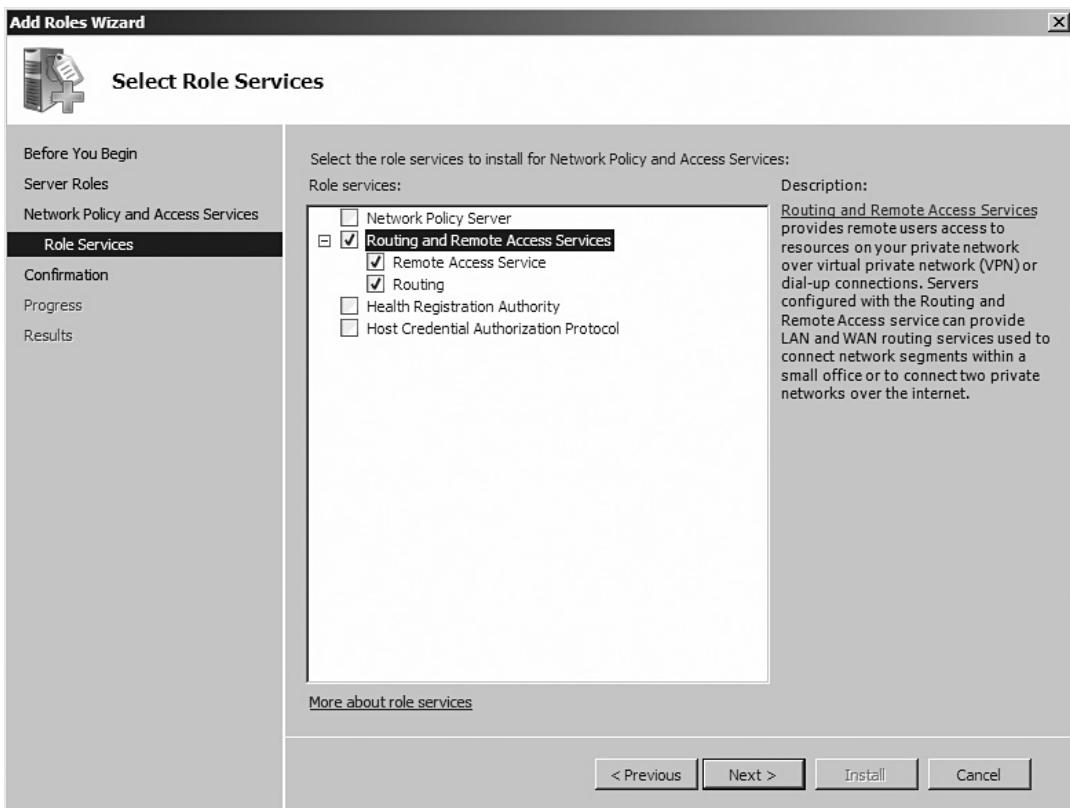
## EXERCISE 4.1

### INSTALLING THE NPAS ROLE WITH THE ROUTING AND REMOTE ACCESS SERVICE

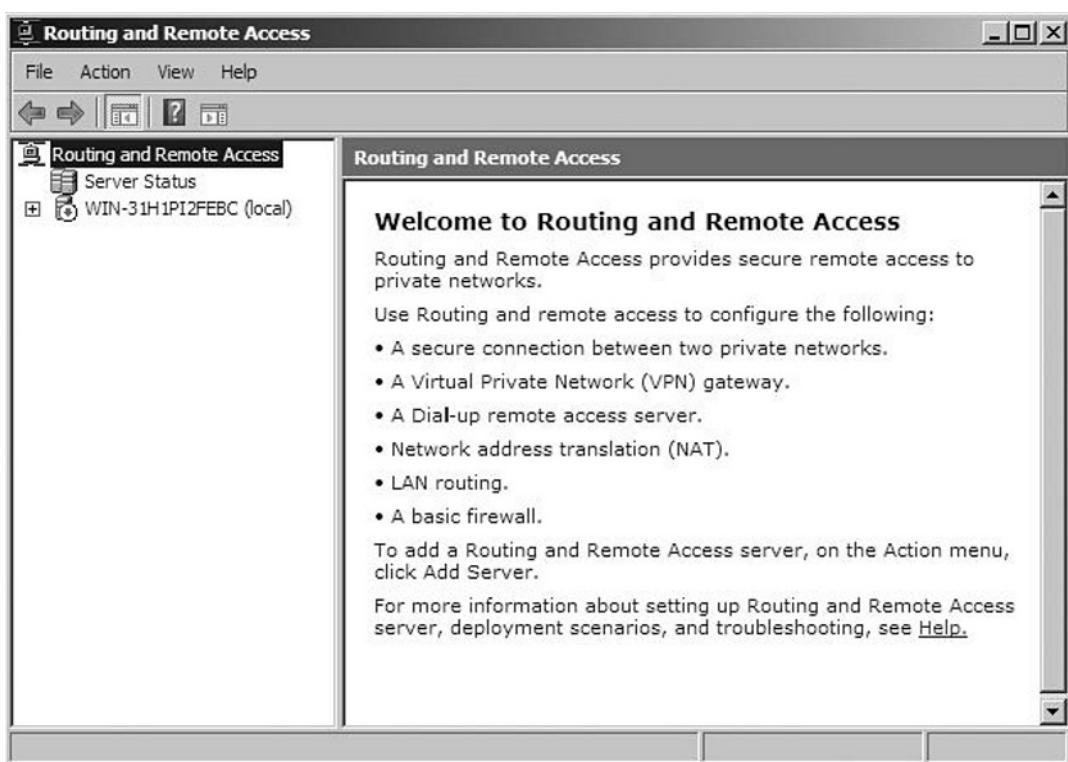
1. Click **Start | Administrative Tools | Server Manager**.
2. Scroll down to Role Summary, click **Add roles**.
3. When the **Before You Begin** page opens, click **Next**.
4. On the **Select Server Roles** page, select **Network Policy and Access Services** (Figure 4.1), and then click **Next**.

**Figure 4.1** Selecting the NPAS Server Role

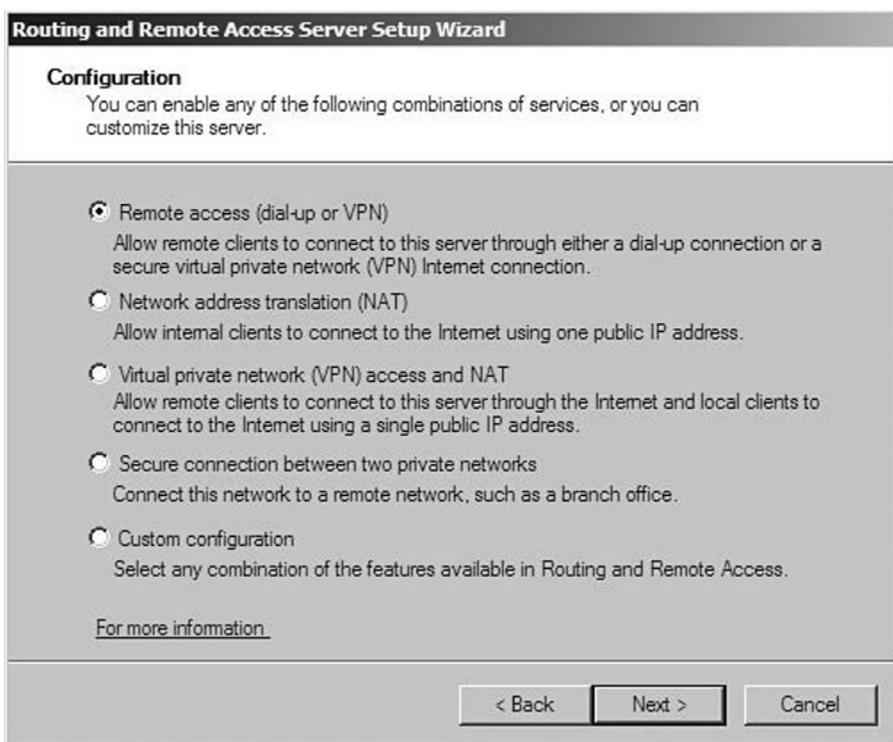
5. Click **Next** again on the **Network Policy and Access Services** page.
6. Next, we need to specify the services we are going to install. We will be selecting **Routing and Remote Access Services**, which will automatically select both the Remote Access Service and Routing service beneath it (Figure 4.2).

**Figure 4.2** Selecting NPAS services

7. On the **Confirm Installation Selections** page, click **Install**.
8. When installation is complete, click **Close**.
9. If the Server Manager window is closed, re-open it. Now that our role has been installed, let's open up the console and view role settings.
  1. Click **Start | Administrative Tools | Routing and Remote Access**.
  2. When the **Routing and Remote Access** window opens, you will notice that the service is disabled (Figure 4.3). To enable the service, right-click on the red down arrow next to the server name and click **Configure and Enable Routing and Remote Access**.

**Figure 4.3** Routing and Remote Access Window

3. At the **Welcome** window, click **Next**.
4. Review the options in the **Configuration** window (Figure 4.4) and click the radio button next to **Custom Configuration**.

**Figure 4.4 Configuration Window**

5. From the **Custom Configuration** window, select **VPN access**, and **LAN routing**. Before clicking **Next**, we recommend clicking the **For more information** hyperlink to view more information about the other options.
6. Click **Finish** to complete the setup wizard.
7. If prompted click **Start service** to start the RRAS service.

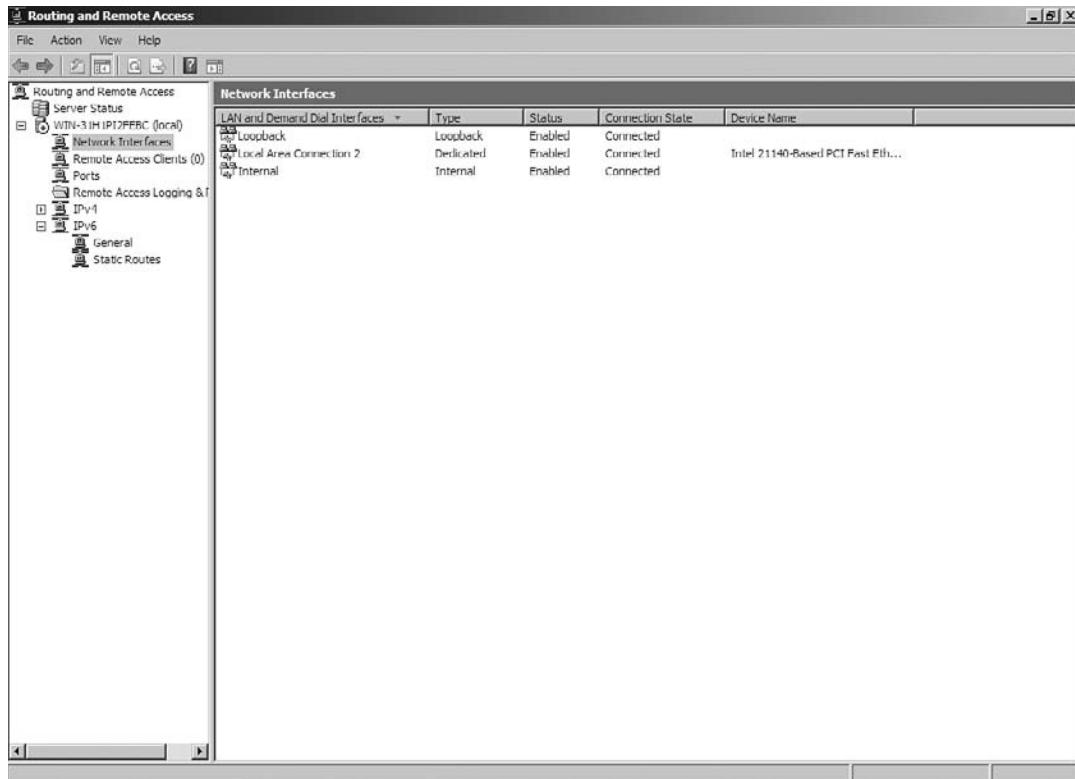
Notice that the red arrow in the RRAS window has changed from red to green and that there are additional options in the tree beneath the server name. Let's discuss each of these options.

## Network Interfaces

To view the available network interfaces, click on the **Network Interfaces** menu option located beneath the server name. Notice that in the right pane, you can see the interfaces, type of interface, and status (Figure 4.5). Though you cannot modify

any of your interfaces through this screen, it gives an at-a-glance view of the NIC configuration. In situations where you may have multiple network cards (or dial-up-networking interfaces for legacy dial-up remote access), this is a great tool to get a snapshot of the environment. It is also helpful in understanding the state of connections, particularly when you are using RRAS for LAN routing.

**Figure 4.5 Network Interfaces Window**



## Remote Access Clients

When RRAS is in use, this window will show the active connections to this RRAS server. When someone is connected, you can right-click on their user name and view details about the connection by clicking on **Status**. Likewise, you can disconnect them from the RRAS server immediately by right-clicking and choosing **Disconnect**.

## Ports

Think about ports the same way you might think about Ethernet ports on a physical network adapter—only that these are virtual ports, and greatly outnumber the amount of physical NICs you can place into a server. If you scroll down the list of ports (Figure 4.6), you will notice that there are three types of ports we discussed earlier in this section—SSTP, PPTP, and L2TP. Let's discuss these different types of ports.

**Figure 4.6** Ports List

The screenshot shows the Windows Routing and Remote Access snap-in. The left pane displays the navigation tree with sections like Server Status, Network Interfaces, Remote Access Clients, Ports, Remote Access Logging & Tracing, IPv4, and IPv6. The right pane is titled "Ports" and contains a table with four columns: Name, Device, Used By, and Status. The "Name" column lists many entries starting with "WAN Minport L (SSTP) (VPN0-)" followed by various port numbers. All entries in the "Used By" column are listed as "RAS", and all entries in the "Status" column are marked as "Inactive".

Name	Device	Used By	Status
WAN Minport L (SSTP) (VPN0-99)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-48)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-47)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-46)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-45)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-44)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-43)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-42)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-41)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-40)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-39)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-38)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-37)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-36)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-35)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-49)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-48)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-47)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-46)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-45)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-44)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-43)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-42)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-41)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-40)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-39)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-38)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-77)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-76)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-75)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-74)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-73)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-72)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-71)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-70)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-7)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-69)	VPN	RAS	Inactive
WAN Minport L (SSTP) (VPN0-68)	VPN	RAS	Inactive

## PPTP

PPTP is a protocol that was, ironically, initially supported by Microsoft as the de facto VPN protocol. PPTP is an extension of an older protocol, known as Point-to-Point Protocol (PPP). PPP uses the IP protocol, and provides layer 2 (data link layer) service. Basically, it packages your computer's TCP/IP packets and forwards them to the server where they can be properly routed to internal resources (or out

to the Internet). For security purposes, PPTP connections are authenticated with Microsoft MSCHAP-v2 or EAP-TLS. Setting up a PPTP connection from a workstation is fairly easy; let's walk through that process now.

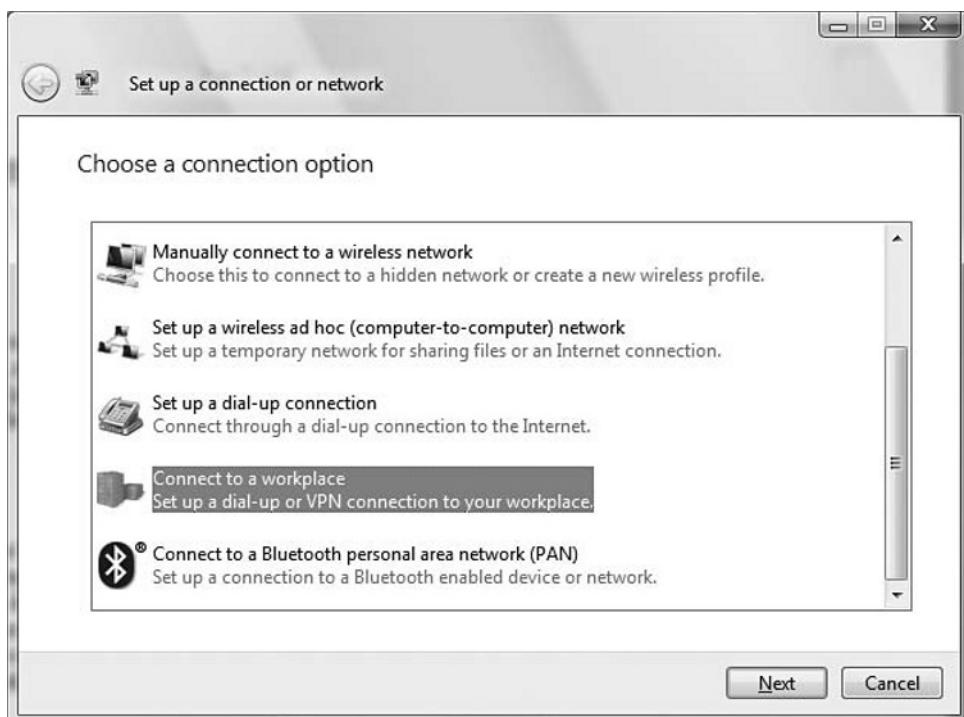
## EXERCISE 4.2

### CONFIGURING A PPTP CONNECTION

We will be configuring this connection from a Windows Vista Enterprise Edition client, however the configuration is very similar as long as you are using a more recent version of the Windows operating system (Windows Vista, Windows XP, Windows Server 2003, Windows Server 2008).

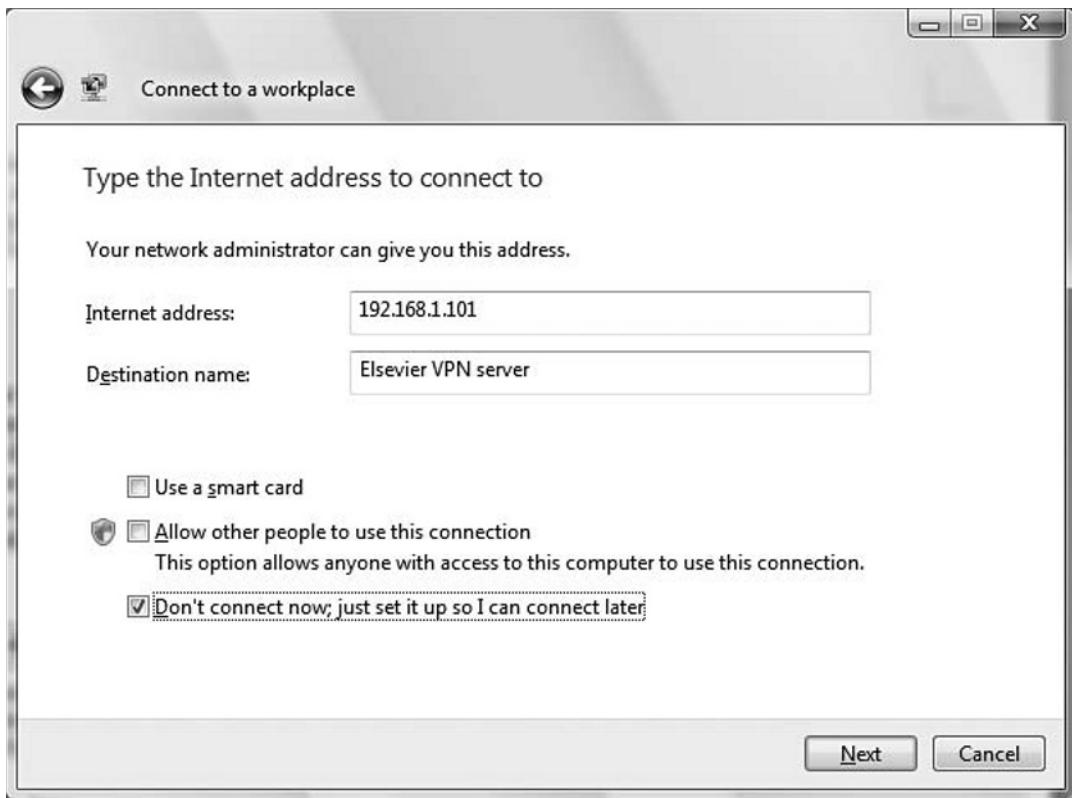
1. Click **Start | Network**.
2. From the top bar, choose **Network and Sharing Center**.
3. From the left pane, choose **Set up a connection or network**.
4. From the **Set up a connection or network** window, choose **Connect to a workplace** (Figure 4.7) and click **Next**.

**Figure 4.7** Set Up a Connection or Network Window



5. When the **Connect to a Workplace** window appears, select **No, create a new connection** and click **Next**.
6. When asked how you want to connect, choose **Use my Internet Connection** and click **Next**.
7. Enter in the IP address of your server in the **Type the Internet Address to connect to** window, name your connection, and check the box next to **Don't connect now** (Figure 4.8).

**Figure 4.8** Type the Internet Address to Connect to Window



8. Click **Next**.
9. Enter in the username and password of your administrator, but leave the domain blank. We will show you how to configure users for remote access on the server later in this chapter. Click **Create**.
10. When the connection is ready to use, click **Close**.

11. Go back to the **Network Sharing Center** and click **Manage Network connections**.
  12. Notice that the new VPN connection appears next to your physical network connections.
- 

## L2TP/IPsec

Layer 2 Tunneling Protocol (L2TP) is a dynamic tunneling protocol which provides for multiple Layer 2 connections to pass across packet-oriented data networks.

The base protocol consists of a control protocol that handles the creation, maintenance and tear-down of the L2TP communication sessions. If it sounds familiar, it is because L2TP is an extension of the PPTP protocol, but combines the PPTP design originated by Microsoft with the L2F protocol designed by Cisco. Unfortunately, L2TP does not provide for data confidentiality and provides little authentication on its own. To aid with this, L2TP and the IPsec protocol have been combined to provide for the need for authentication and confidentiality.

Creating an L2TP connection is as simple as creating the PPTP connection in Exercise 4.02. By default, the VPN connection type is set to “Automatic,” but can be changed to either PPTP or L2TP/IpSec exclusively. These settings are found in the **Network** tab of the connection properties after the connection has been created in Exercise 4.02.

## SSTP

Secure Socket Tunneling Protocol (SSTP) is a further evolution of VPN tunneling. SSTP is used to encapsulate the PPP traffic inside the more commonly-used Secure Sockets Layer (SSL) protocol—commonly used in secure Web sites. As we mentioned earlier, Microsoft has continued to make a push to using SSL as the de facto standard for remote communications, and SSTP is another example of this. .

### NOTE

---

It is important to note that the SSTP protocol is only supported in Vista SP1 and Windows Server 2008 as of the writing of this book.

---

## Network Access Protection

Microsoft for some time has been making security its main priority with the Microsoft Trustworthy Computing initiative. Starting with Microsoft Windows Server 2003 we were introduced to Network Access Quarantine Control. This feature enabled administrators to control remote access to a private network until the remote computer was validated by a script. The components necessary to deploy Network Access Quarantine Control included Microsoft Windows Server 2003 Routing and Remote Access Service (RRAS), the Connection Manager Administration Kit (CMAK), and Internet Authentication Service (IAS).

The most obvious problem with Network Access Quarantine Control was that it worked with only remote computers connecting to the network using Microsoft's Routing and Remote Access Services (RRAS). This solution left a wide gap throughout the network infrastructure for other (non-Microsoft) types of clients to cause issues and management problems for network administrators.

With Microsoft Windows Server 2008, Windows Vista, and Windows XP Professional Service Pack 3, Microsoft has introduced Network Access Protection (NAP). NAP can control virtual private network (VPN) connections better than Network Access Quarantine Control, but NAP can also enforce policy compliance through the following types of network access or communications:

- Internet Protocol security (IPsec) protected traffic
  - IEEE 802.1x authenticated network connections
  - Dynamic Host Configuration Protocol (DHCP) address configurations
- Remote access VPN connections

The key word to keep in mind when discussing NAP and its features is “compliance.” With the introduction of NAP into our network, we can force Windows Server 2008, Windows Vista, and Windows XP Professional Service Pack 3 to comply with standards set forth on our network. If for some reason a client does not comply with standards set forth by an administrator, the client could be directed to a separate network segment. On the separate network segment, a Remediation Server could update the client to the company’s standards and then allow the client access to the network. Examples of these standards include but are not limited to:

- Windows update files
- Virus definitions
- Windows firewall settings

In addition, Microsoft has provided an Application Program Interface (API) so that Network Access Protection partners can write their own piece of software to add to the functionality of NAP. Some of the Access Protection partners already providing add-ons include AppSense, Citrix, Intel, and Symantec. For a complete list of Access Protection partners, go to the following Web site: [www.microsoft.com/windowsserver2008/en/us/nap-partners.aspx](http://www.microsoft.com/windowsserver2008/en/us/nap-partners.aspx).

In the following section, we are going to first look at all of the components of implementing NAP on a network. Once we gain a broad understanding of the components needed to build a NAP-supported network, we will look at different scenarios and implementation steps through the exercises throughout this chapter.

## Working with NAP

The NAP platform main objective is to validate the state of a client computer before connecting to the private network and offer a source of remediation. To validate access to a network based on system health, NAP provides the following areas of functionality:

- Health state validation
  - Network access limitation
  - Automatic remediation
- Ongoing compliance

### TEST DAY TIP

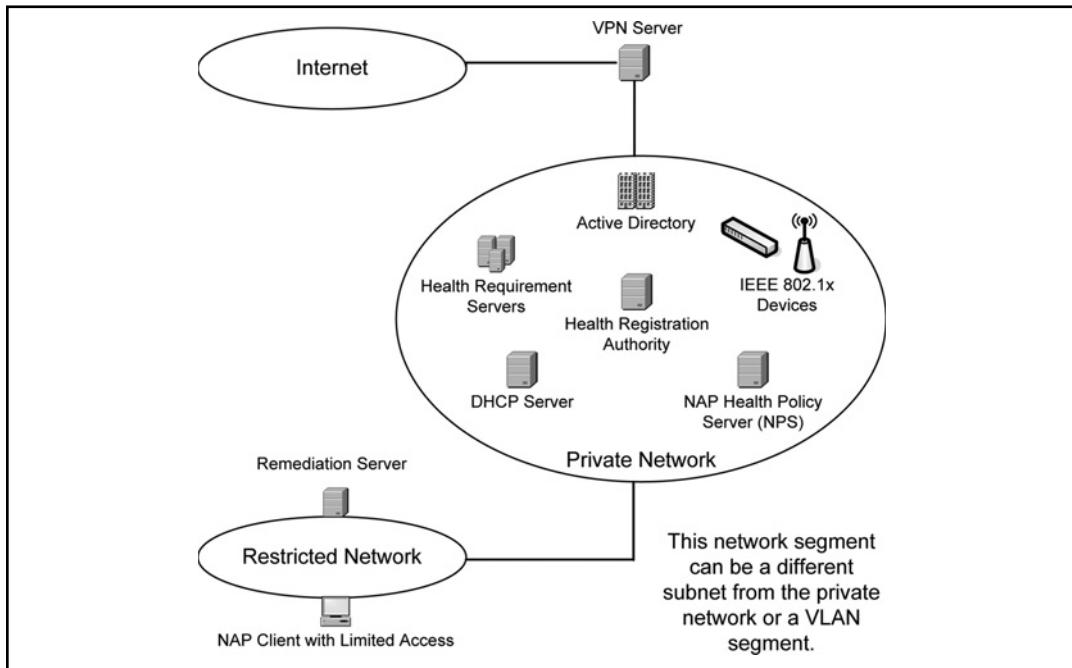
It would be advisable to look over the bullet points listed in this section before going into the exam. Although the exam is technical in nature, the agents provided by Microsoft provide the aforementioned validations for Windows Server 2008, Windows Vista, and Windows XP Professional Service Pack 3. Other validation types will be provided by third-party vendors.

### *Network Layer Protection*

All the components of NAP reside at the network layer. It is very important to understand where each component can reside and what the function of each component does. We are first going to look at a very general Microsoft Visio

drawing and then point out each component and its function as related to NAP. Like a lot of Microsoft network designs, some servers can play multiple Windows Server 2008 roles within the NAP-enabled network architecture. Later in this chapter we will point out during the hands-on exercises where these servers with multiple Windows Server 2008 roles can reside, but for now we will concentrate on each individual function of the components and server roles (see Figure 4.9).

**Figure 4.9** NAP Network Design



## NAP Clients

NAP clients can be Windows Vista, Windows Server 2008, or Windows XP Service Pack 3 clients. At the time of this writing these are the only operating systems that support the NAP platform for system health validated network access or communication. Microsoft does plan on supporting other operating systems through third-party software providers, typically named Independent Software Vendors (ISVs).

Microsoft is also planning to provide support to the Microsoft Windows Mobile platform, including support for handheld devices and Microsoft Windows Mobile phones.

The NAP API is really important for the adoption of NAP-based networks. The API that Microsoft is releasing for developers allows them to write code to support various other clients that are not Microsoft based. Expect to see these devices become more popular as more and more enterprises adopt Microsoft Windows Server 2008.

## NAP Enforcement Points

NAP enforcement points are parts of the NAP infrastructure that determines the health and compliance of a NAP client before allowing network access. To determine if the NAP client is in compliance by the policies set forth by the administrator, the NAP Health Policy Server (NPS) evaluates the health and compliance of the NAP client. The NPS also decides the remediation process that is going to be applied to the NAP client. For instance, the client can be forwarded to a restricted network where a remediation server will offer the updates or settings needed to enforce the compliance policy. NAP enforcement points include the following:

- **Health Registration Authority (HRA)** The HRA is a Windows Server 2008 with the roles of Internet Information Server 7.0 (IIS) and Certificate Authority (CA) role installed. This enforcement point is used primarily with IPsec Enforcement policies. The CA uses health certificates to enforce NAP compliance to the NAP client.
- **Windows Server 2008 VPN Server** A server running Windows Server 2008 Network Policy Server can enforce NAP compliance to a NAP client.
- **DHCP Server** Servers installed into the NAP network infrastructure running Windows Server 2008 with the DHCP server role providing Internet Protocol version 4 (IPv4) addresses to NAP clients can enforce NAP compliance to a NAP client.
- **Network access devices** Network hardware, such as switches and wireless access points that support IEEE 802.1 x authentication, can be used to support NAP compliance to a NAP client. Types of protocols supported include Extensible Authentication Protocol (EAP), Lightweight Extensible Authentication Protocol (LEAP), and Protected Extensible Authentication Protocol (PEAP).

**EXAM WARNING**

During the examination, Microsoft sometimes like to give you scenario questions and ask what it is that is wrong with the provided solution. One of the multiple choice answers could be none—meaning the solution is correct on its own merit. At face value this may be correct. For example, a scenario question may include the addition of a DHCP server running Internet Protocol version 6 (IPv6) in a NAP client. Windows Server 2008 does support IPv6; however, NAP does not support IPv6, only IPv4. Make sure you read the scenario in its entirety and pay close attention to detail.

## Active Directory Domain Services

As you already know, Active Directory Services store account and group policy information for an Active Directory Domain. NAP does not necessarily rely on Windows Server 2008 Active Directory Domain Services or Windows Server 2003 Active Directory Domain Services. NAP definitely does not need Active Directory Services to determine if a client is compliant, but other services and roles depend on Active Directory Services.

Active Directory Domain Services is needed for Network Policy Server VPN enforcement, IEEE 802.1x network device enforcement, or IPsec-based enforcement. Also, as you will see later in this chapter, using group policy objects is a good way to set compliance and enforcement settings to NAP clients on your network.

## NAP Health Policy Server

The NAP Health Policy Server is the heart of the NAP-supported network infrastructure. The NAP Health Policy Server runs Windows Server 2008 and has the NPS server role installed. The NPS server role is responsible for storing health requirement policies and provides health state validation for NAP.

Interestingly, the NPS server role replaces Internet Authentication Service (IAS), Remote Authentication Dial-In User Service (RADIUS), and proxy server provided by Windows Server 2003. So, NPS not only supports the NAP infrastructure but also acts as the Authentication, Authorization, and Accounting (AAA) server in Windows Server 2008. The NPS role can act as the RADIUS proxy to exchange RADIUS data packets with another NAP health policy server.

## Head of the Class...

### Additional Information about AAA Services

The following definitions are provided to help you better understand exactly what the AAA services provide:

- **Authentication** Authentication refers to the process of establishing the digital identity of one entity to another entity. Commonly one entity is a client (a user, a client computer, etc.) and the other entity is a server (computer). Authentication is accomplished via the presentation of an identity and its corresponding credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).
- **Authorization** Authorization refers to the granting of specific types of privileges (including “no privilege”) to an entity or a user, based on their authentication, what privileges they are requesting, and the current system state. Authorization may be based on restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user. Most of the time the granting of a privilege constitutes the ability to use a certain type of service. Examples of types of service include, but are not limited to: IP address filtering, address assignment, route assignment, QoS/differential services, bandwidth control/traffic management, compulsory tunneling to a specific endpoint, and encryption.
- **Accounting** Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended.

## Health Requirement Server

Health requirement servers contain the data that NAP NPS servers check for current system health state for NAP NPS servers. Examples of the data that health requirement servers may provide are the latest virus DAT information files for third-party antivirus packages or updates for other software packages that the ISVs use the NAP API to develop.

## Restricted Network

A restricted network is where NAP sends a computer that needs remediation services or to block access to the private network until remediation can take place. The restricted network can be a different subnet that has no routes to the private network or a different logical network in the form of a virtual local area network (VLAN). A good NAP design would place remediation servers located within the restricted network. Placing remediation servers inside the restricted network enables NAP clients to get updated and then be allowed access to the private network.

The remediation server could be in the form of a Windows Server 2008 or Windows Server 2003 running Windows Server Update Services (WSUS). WSUS provides an easy way to update the NAP client system files using Microsoft Update Services. You could also place virus update files and other third-party critical update files on the remediation server.



### TEST DAY TIP

---

A good review on the test date is to go through this book and look over the diagrams and understand how to interpret different network designs. Glancing over these network diagrams is a good refresher right before entering the testing center.

---

## Head of the Class...

### Understanding VLANs

When you are working with NAP, one of the best technologies to take advantage of is working with virtual local area networks also known as VLANs. Microsoft does not go into great detail about how VLANs work, but for any student or a well-seasoned network administrator, understanding this technology is vital. Without VLANs in place, management of even the smallest network can become quite ugly due to the amount of broadcast traffic that can occur between connected systems. VLANs are vital to preventing unnecessary network “chatter” through segmentation of networks and systems.

VLANs are basically the logical grouping of multiple network segments (or subnets) on the same switch. The switching management software allows us to take ports from the switch and build multiple virtual local area networks that can span not only the switch you are configuring, but other switches on your network as well. These virtual networks are independent of each other.

Layer 3 (Network Layer) switches allow us to configure routing between these VLANs because there is a router module installed within the typical Layer 2 switch that allows packets to be forwarded from subnet to subnet at wire speed. This adds security, speed, and flexibility to your network design.

The way it helps with NAP is that VLANs allow us to create the remediation network that is necessary for temporary segmentation of systems that do not currently meet the health requirements of the organization.

This makes setting up the restricted network in NAP easy and more efficient.

To read more about VLAN technology, go to this Web address: [www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2023.htm#wp3280](http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2023.htm#wp3280).

## Software Policy Validation

Before you actually start doing some exercises, it is important to understand what actually goes on during system-compliant testing and validation. NPS uses System Health Validators (SHVs) to analyze the compliance of a client computer.

SHVs determine whether a computer is getting full access to the private network or if it will be isolated to the restricted network. The client has a piece of software installed called a System Health Agent (SHA) to monitor its system health. NPS uses SHVs and SHAs to determine the health of a client computer and to monitor, enforce, and remediate the client computer.

Built into Windows Server 2008 and Windows Vista are the Windows Security Health Agent (WSHA) and Windows Security Health Validator (WSHV). The Health Agent resides on the client-side (Vista), while the Validator resides on the server-side (Windows Server 2008).

These agents are used to enforce the most basic compliance settings in a NAP infrastructure. The settings provided by WSHA and WSHV are:

- The client computer has firewall software installed and enabled.
- The client computer has antivirus software installed and enabled.
- The client computer has current antivirus updates installed.
- The client computer has antispyware software installed and enabled.
- The client computer has current antispyware updates installed.
- Microsoft Update Services is enabled on the client computer.

Even without third-party SHVs and SHAs, Microsoft has built very powerful tools into Windows Server 2008, Windows Vista, and Windows XP Professional Service Pack 3 to validate the compliance and health of computers.

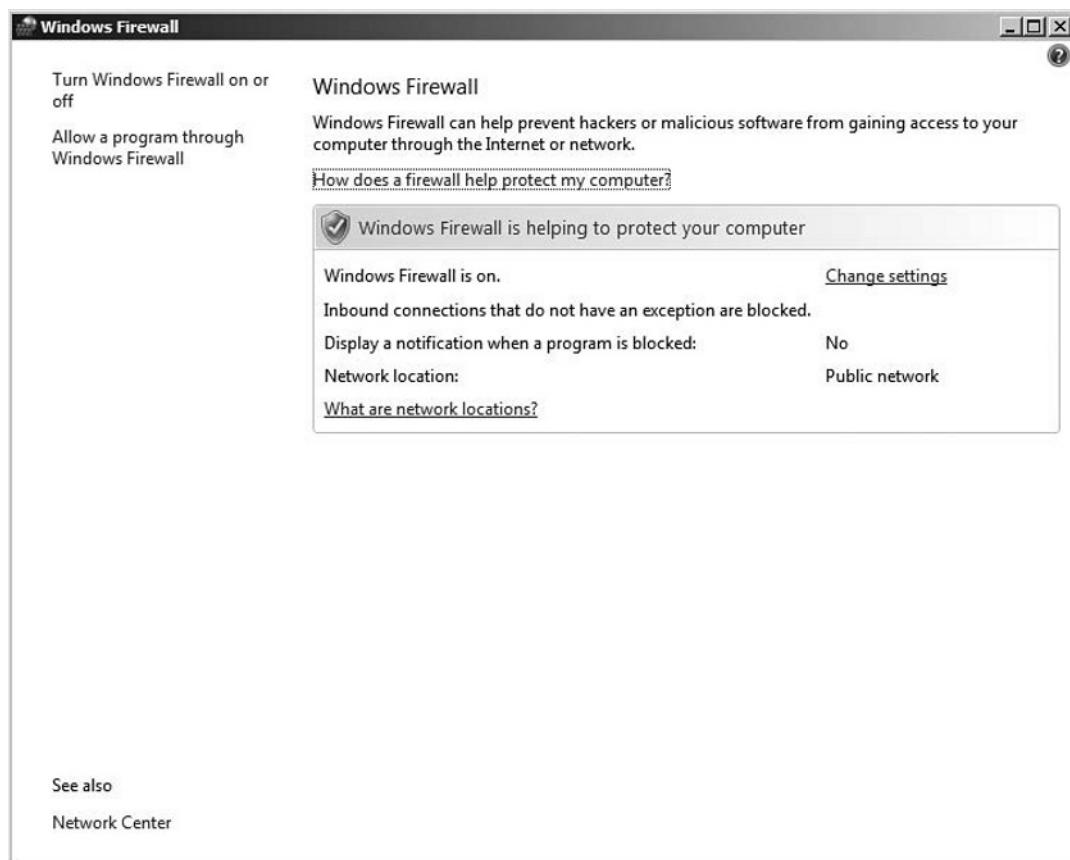
## Server Security

By their very nature, servers are intended to be used for the access of data and/or resources by multiple people in multiple ways. Because servers are intended to be accessed in this way, security can quickly become an issue. Security for a server needs to be addressed at both a physical and technical (or logical) level. While Windows Server 2008 cannot necessarily address the physical security issue (it can help with preventing copying of data to removable media, but won't help you to move the server to a secured room), it can certainly provide tools to help address the technical aspects of server security. In this section, we will discuss some of the advancements to the Windows Firewall solution, as well as the introduction of volume-level encryption of data.

## Windows Firewall Management

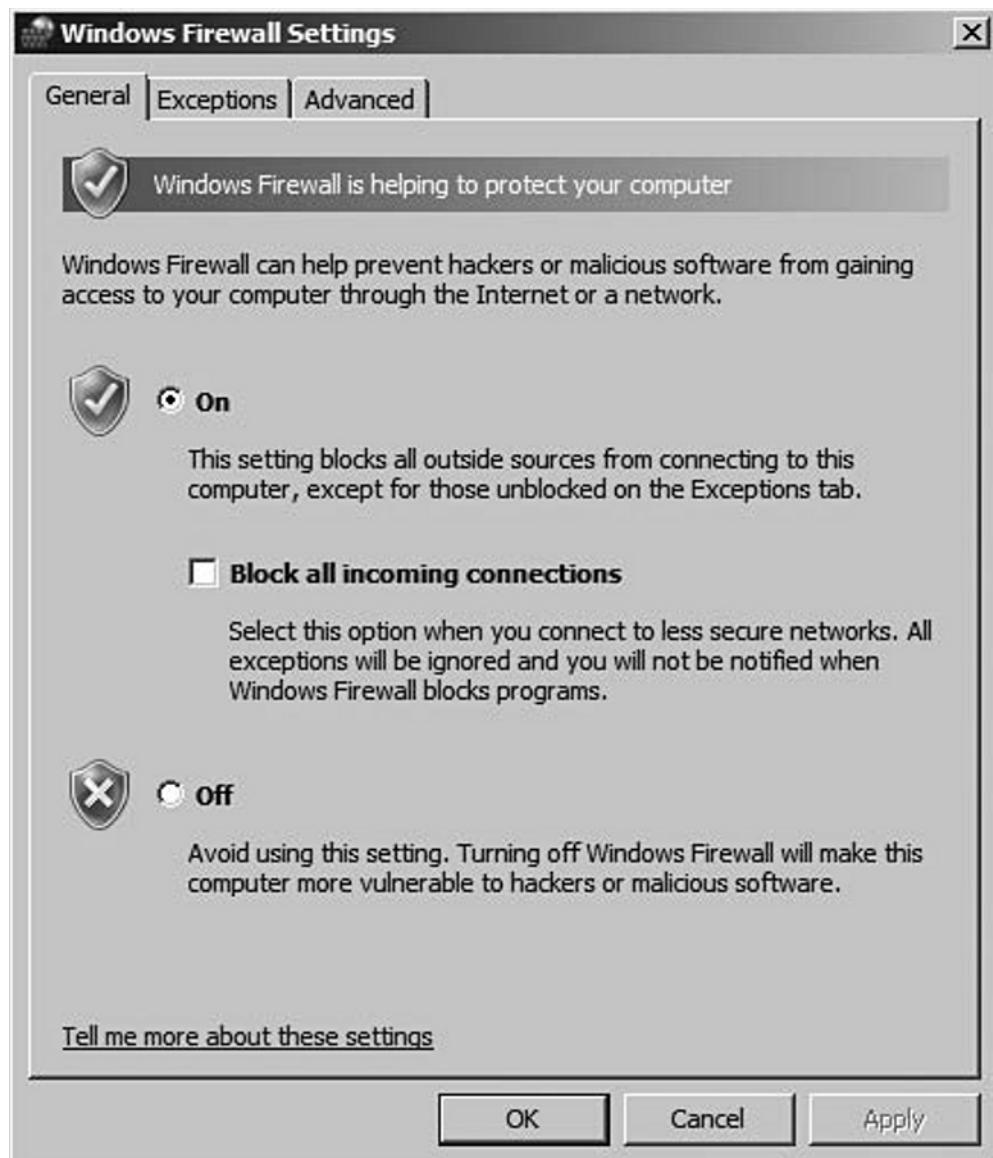
Similar to the Windows Vista firewall, the Windows Firewall with Advanced Security is a stateful, host-based firewall that you can configure to allow or disallow traffic that is generated by either a particular executable file, such as C:\Program Files\Microsoft SQL Server\sqlserver.exe, or traffic that is destined for one or more TCP or UDP ports, such as TCP port 80 for Hypertext Transfer Protocol (HTTP) traffic. You'll find that basic firewall configuration tasks haven't changed much between Windows XP and Windows Vista; you'll continue to make these changes using the Windows Firewall Control Panel applet. But even this piece has been updated to make it more intuitive and informative for the end user: When you open the Windows Firewall applet, the first thing you see is a summary of your current Windows Firewall settings, as shown in Figure 4.10.

**Figure 4.10** A New Look for the Windows Firewall Control Panel Applet



As you can see, this provides an at-a-glance summary of the current state of the firewall; whether it is turned on or off, how exceptions and notifications are being handled, and the network location to which the computer is currently connected. By clicking on **Change settings**, you'll be taken to a familiar-looking interface that will actually allow you to make changes, as shown in Figure 4.11.

**Figure 4.11** Configuring Basic Windows Firewall Settings



Similar to Windows XP, we define the three settings on the General tab as follows:

- **On (recommended)** This is the recommended setting and is enabled by default when Vista is installed. This will block any unsolicited incoming communication attempts that are made against the Vista workstation. All outbound traffic will still be permitted, and any inbound responses to outbound traffic that was initiated by the user will also be permitted. On the Exceptions tab, you can still define exceptions for inbound traffic that should be permitted.
- **Block all incoming connections** By placing a checkmark here, you will instruct the Windows Firewall to block all unsolicited connection attempts even if exceptions are defined on the Exceptions tab. You should select this option if you are connected to a public or otherwise insecure network such as one in a hotel, airport, or coffee house, or if a known virus or worm is spreading across the Internet and you want to be extra careful until the threat has largely run its course. When you remove the checkmark next to this option, any traffic defined on the Exceptions tab will once again be permitted to connect to the Vista workstation.
- **Off (not recommended)** Microsoft does not recommend this setting for obvious reasons, as it leaves the workstation vulnerable to hackers and malicious software. The only reason you might want to turn off the Windows Firewall would be if you or your organization has already standardized on a third-party software firewall such as the ones offered by Symantec, McAfee, and others.

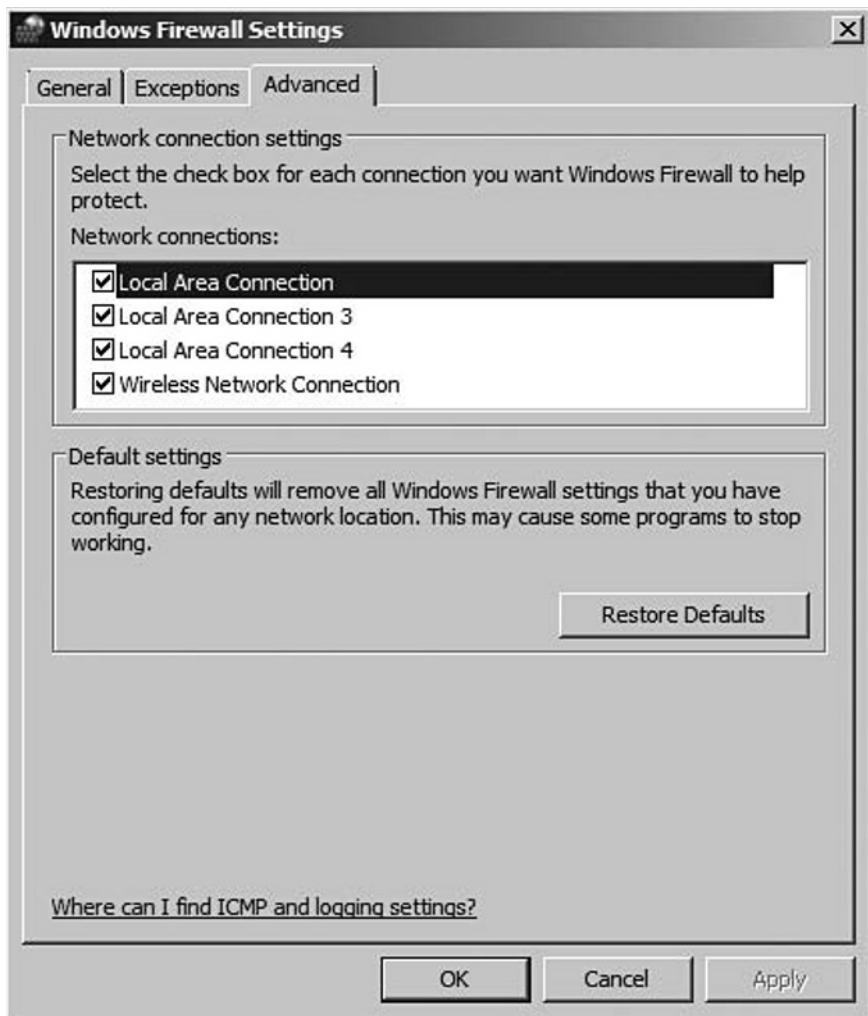
The Advanced tab in the Control Panel applet has had most of its functionality removed relative to Windows XP SP2. In XP SP2, the Advanced tab allowed you to configure settings for firewall logging, allowing or disallowing inbound ICMP traffic, and creating exceptions on a per-interface basis. As you can see in Figure 4.12, the Advanced tab in the Vista firewall only allows you to do the following:

- Enable or disable the firewall on each installed network interface
- Restore the Windows Firewall to its default settings

**NOTE**

The functions that were formerly found on the Advanced tab, as well as a number of new features in the Windows Server 2008 firewall, have been moved to the Windows Firewall with Advanced Security MMC snap-in, which we'll discuss in the following section.

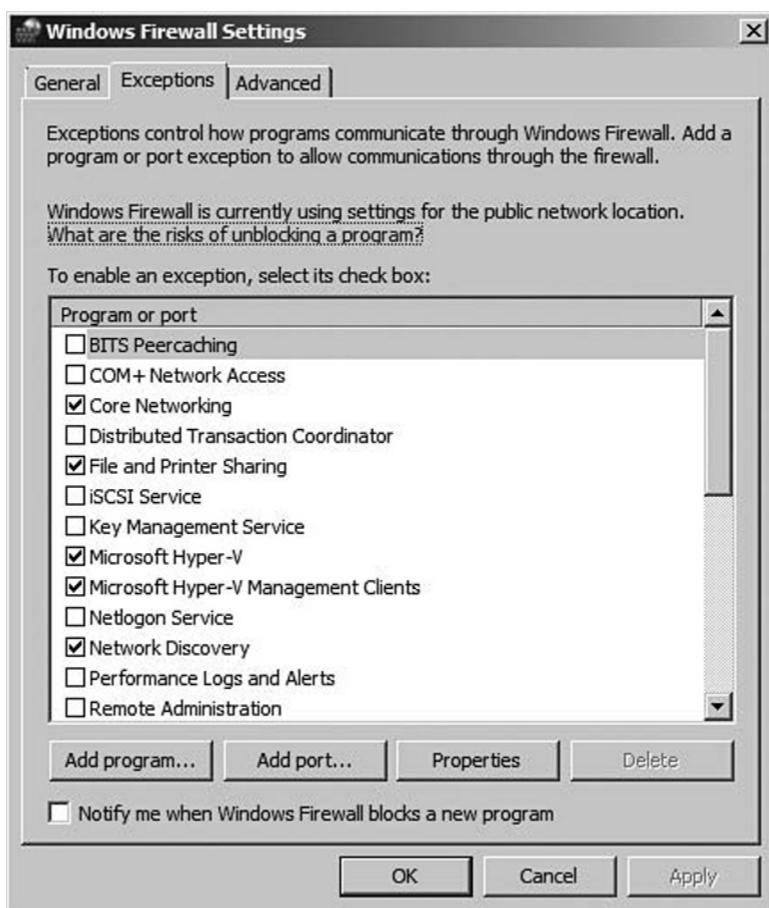
**Figure 4.12** The Advanced Tab in the Windows Server 2008 Firewall



## Working with Built-in Firewall Exceptions

In Figure 4.13, you can see the Exceptions tab of the Windows Firewall Control Panel applet. Windows Server 2008 has improved this tab by offering a much wider array of preconfigured firewall exceptions, including the following:

**Figure 4.13** Viewing the List of Windows Firewall Exceptions



- **BITS Peercaching** Allows workstations in the same subnet to locate and share files from the Background Intelligent Transfer Service (BITS) cache using the WSDAPI framework.
- **Core Networking** This allows for basic inbound and outbound network connectivity over wired and wireless connections.

- **Distributed Transaction Coordinator** Coordinates transactions that update transaction-protected resources such as databases, message queues, and file systems.
- **File and Printer Sharing** Used for sharing local files and printers with other users. File and Printer Sharing still relies on NetBIOS, SMB, and RPC to communicate.
- **iSCSI Service** Used for connecting to iSCSI target servers and devices.
- **Media Center Extenders** Allows Media Center Extenders to communicate with a computer running Windows Media Center.



### NOTE

---

The exceptions for the Microsoft Office and MSN Messenger products that you see in Figure 6.16 are not default exceptions that come with Windows Vista; these exceptions were configured automatically by the Office and Messenger installation routines.

---

- **Network Discovery** As we discussed earlier in this chapter, this feature allows a Windows Vista device to discover other devices and be discovered by other devices on the network using SSDP, Universal Plug and Play, NetBIOS, and LLMNR.
- **Remote Administration** This allows administrators to connect remotely to the local computer using interfaces such as the Computer Management MMC snap-in, as well as familiar administrative hidden drive shares such as \\computername\c\$.
- **Remote Desktop** Allows a remote user to connect to the Vista desktop using the Remote Desktop client over TCP port 3389.
- **Remote Event Log Management** Allows remote viewing and management of the local event log using Named Pipes and RPC.
- **Remote Scheduled Task Management** Allows remote management of the local task scheduling service over RPC.
- **Remote Service Management** Allows remote management of local services using Named Pipes and RPC.

- **Remote Volume Management** Provides the ability to manage software and hardware disk volumes remotely over RPC.
- **Routing and Remote Access** Creates exceptions to allow incoming VPN and Remote Access Server (RAS) connections.
- **Telnet and Telnet Server Remote Administration** Creates a firewall exception to allow remote administration using telnet on TCP port 21.
- **Windows Collaboration Computer Name Registration Service** Allows other computers to locate and communicate with the local computer using the Peer Name Resolution Protocol and SSDP.
- **Windows Firewall Remote Management** Allows for remote management of the Windows Firewall over RPC.
- **Windows Management Instrumentation (WMI)** Allows system administrators to retrieve and modify configuration information about the local PC using a standard set of classes and components.
- **Windows Remote Management** Allows remote management of a Vista system using WS-Management, which is a Web services-based protocol that allows for remote management of operating systems and devices.
- **Wireless Portable Devices** Allows users to transfer media from a networked camera or other media device using the Media Transfer Protocol (MTP). This exception relies on UPnP and SSDP to function.

## Creating Manual Firewall Exceptions

In addition to the built-in firewall exceptions we just discussed, you can also create additional firewall exceptions to allow inbound traffic to pass through the Windows Firewall. In many cases, these manual exceptions will be created automatically by the installer for a particular program, or else you'll need to manually specify them from the Exceptions tab. The two types of exceptions you can create are as follows:

- **Port exceptions** These exceptions allow all incoming traffic destined for particular TCP or UDP ports; for example, you can create an exception to allow incoming traffic on TCP port 80 for HTTP traffic, or on UDP port 69 for Trivial File Transfer Protocol (TFTP) traffic.
- **Program exceptions** These exceptions allow all incoming traffic that is destined for a particular executable file running on the local workstation, which will typically correspond to a service running on the local computer. To understand the difference between a port exception and a program

exception, let's look at the example of creating an exception for sqlserver.exe, the executable file associated with Microsoft SQL Server, versus opening an exception for TCP port 1433, which is the default TCP port that SQL Server uses. By creating an exception for sqlserver.exe, the Windows Firewall will allow incoming traffic only when the SQL Server service is actually running; if you stop the service to perform an application upgrade or database maintenance, the Windows Firewall will not accept incoming Structured Query Language (SQL) traffic while the application is not running. By contrast, creating a port exception for TCP 1433 will create an "always on" exception; the Windows Firewall will accept traffic from port 1433 regardless of whether the SQL Server service is running.

## EXERCISE 4.3

### MANUALLY CREATING A FIREWALL EXCEPTION

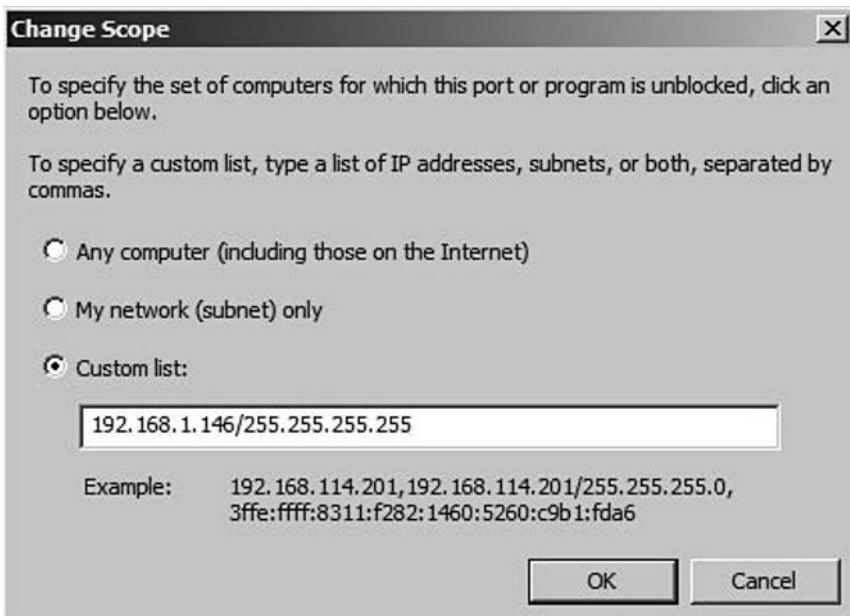
In this exercise, we will walk through the process of creating a manual firewall exception.

1. To create a program exception, click on **Add program** from the **Exceptions** tab. Click on **Browse** to select the executable file for which you want to create an exception and then select **Open**. In our example, we will use calc.exe, which is located in <local-drive>:\windows\system32.
2. To restrict the scope of an exception that you've created, click on the **Change scope** button. You'll be presented with the screen shown in Figure 4.14, which will allow you to set one of the following three scopes:
  - **Any computer (including those on the Internet)** This scope will allow any computer on any network to access this program, including computers located anywhere on the Internet.
  - **My network (subnet) only** For example, if your workstation has an IP address of 192.168.1.100 and a subnet mask of 255.255.255.0, the exception will be accessible by a machine with an IP address of 192.168.1.1 through 192.168.1.254.
  - **Custom list** Here you can specify a list of individual IP addresses or ranges and their associated subnet masks; separate multiple entries with commas. For example, you can allow an exception

for an entire range of clients plus an administrative workstation as follows: 192.168.1.146/255.255.255.255, 192.168.2.0/255.255.0. Unfortunately, there isn't a good way to specify a range of addresses that does not correspond to a subnet mask; if you want to allow an exception for 192.168.1.152 through 192.168.1.159, you will need to specify each IP address individually.

3. Click **OK** twice to close the exception windows.

**Figure 4.14** Configuring the Scope of an Exception

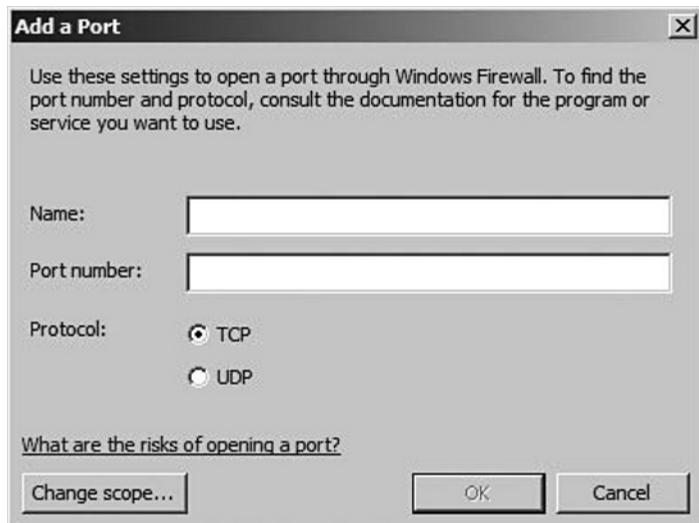


### TEST DAY TIP

Use the **My network (subnet) only** scope with care if you are creating an exception for a computer that is attached to a home-based ISP using a cable modem or DSL connection. Depending on the way in which your ISP has configured its network, using this exception on a home network might open up the firewall exception not just to every machine on your home network, but to every machine in a much larger portion of the ISP's customer base.

4. To create a port exception, you'll likewise click the **Add port** button when creating the exception; you'll see the screen shown in Figure 4.15. Creating a port exception requires the following information:
  - **Name** A descriptive name for the exception, such as "HTTP," "Windows Server Update Services (WSUS) Administration Port," and so on.
  - **Port** The port number of the exception.
  - **TCP/UDP** Whether the exception corresponds to a TCP port or a UDP port.
  - **Scope** By clicking the **Change scope** button, you'll specify the scope of the exception just as you would for a program exception.
5. When you have created your port exception, click **OK** to close the window.

**Figure 4.15** Creating a Port Exception



## Advanced Configuration of the Windows Firewall

Unlike the Windows Firewall in XP SP2, you cannot modify the scope or properties of the preconfigured Windows Server 2008 exceptions from the Control Panel applet. However, there is a new interface for more advanced configuration of the firewall through an MMC snap-in, called Windows Firewall with Advanced Security. This new snap-in provides a number of new features that were not previously available in the XP firewall, including the following:

- Controlling outbound as well as inbound traffic. The inability to control outbound traffic was a major criticism of the Windows Firewall in XP SP2, which was limited in functionality to controlling inbound traffic only.
- Configuring the Windows Firewall on remote computers. This feature allows you to attach to a remote computer and configure the firewall from within the Windows Firewall with an Advanced Security snap-in.
- Integrating Windows Firewall functionality with IPsec. You can now control and administer both of these features from within the same MMC snap-in to avoid conflicts between them.
- Configuring Authenticated IPsec Bypass, a feature that allows IPsec-authenticated computers to bypass firewall rules that would otherwise block incoming or outgoing connection attempts.
- Creating and configuring separate firewall profiles based on whether a computer is attached to a private network or a corporate domain versus attaching to a public network in an airport, coffee shop, and the like. The XP SP2 firewall allowed for only two profiles—Domain and Standard—which did not allow the level of granularity that is often required for mobile computers and traveling workers.

You can access the new Windows Firewall with Advanced Security applet from the Administrative Tools menu, or by opening a blank MMC console and clicking on **File | Add/Remove Snap-In**. You can see the opening screen of the new snap-in in Figure 4.16. As you can see, this snap-in provides a very different view of the Windows Firewall. The left-hand and right-hand panes provide you quick access to perform common tasks and to access different portions of the snap-in, such as viewing inbound rules, outbound rules, connection security rules, and firewall monitoring.

**Figure 4.16** Viewing the Windows Firewall with Advanced Security MMC Snap-In



The main screen of the snap-in provides an at-a-glance view of the three available firewall profiles, as well as a visual indicator of which profile is active. The Windows Server 2008 firewall allows you to create different firewall settings for the following profiles:

- The Domain Profile is active whenever the computer is attached to a corporate Active Directory domain.
- The Private Profile is active when the computer is attached to a private network.
- The Public Profile is active when the computer is attached to a public network.

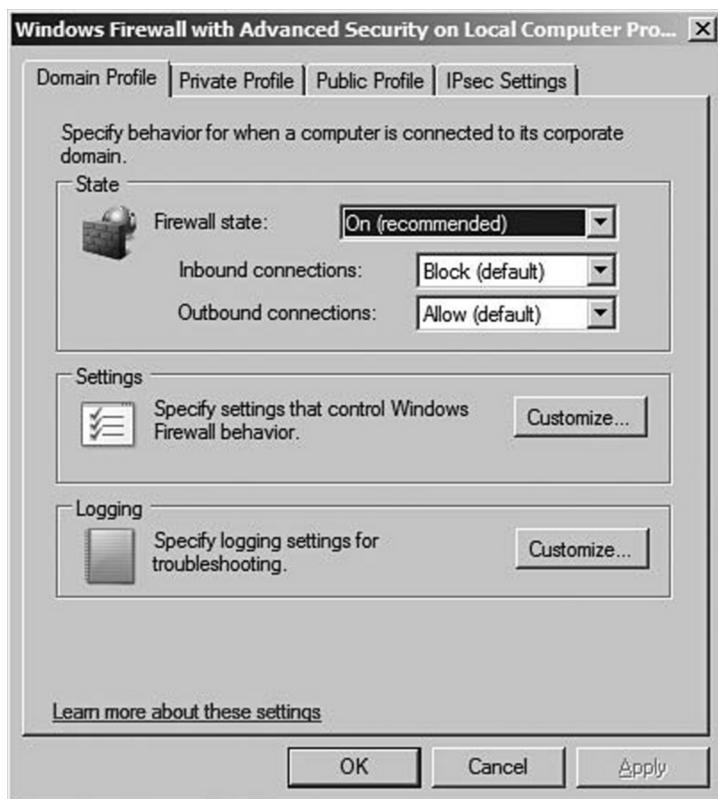
As you can see from Figure 4.16, the default Windows Firewall settings are similar for all three profiles: The Windows Firewall is turned on, inbound connections that do not have a defined exception are blocked, and all outbound traffic is permitted. To customize this default behavior for one or more profiles, click on the **Windows Firewall Properties** link; you'll see the screen shown in Figure 4.17. From here, you can change the firewall state from on to off, and change the behavior

for inbound and outbound connections. You can change the behavior for inbound connections to one of the following:

- **Block** Blocks any inbound connection attempt that doesn't have an exception associated with it. This is the default setting for inbound connections on all three profiles.
- **Block all connections** Blocks all incoming connection attempts regardless of whether there is a rule associated with them; this corresponds to the **Block all incoming connections** checkbox in the Windows Firewall Control Panel applet.
- **Allow** This setting allows any inbound connection attempt.

You can set the behavior for outbound connections to **Allow** (the default for all three profiles) or **Block**, which will block outbound traffic unless a rule has been created to allow it.

**Figure 4.17** Customizing Windows Firewall Settings



Clicking **Customize** under the **Settings** header will allow you to configure the following:

- Whether to display a notification when Windows Firewall blocks an incoming connection. By default, notifications are enabled in all three profiles.
- Whether to allow a unicast response to broadcast or multicast traffic. This is permitted by default in all three profiles. Disabling this feature will not interfere with the operation of a DHCP server, as the Windows Firewall will always permit responses to DHCP messages. However, disabling this feature will interfere with many network discovery protocols, such as NetBIOS, SSDP, and WSDAPI.

Clicking **Customize** under the **Logging** header will allow you to configure these settings:

- The name, size, and location of the Windows Firewall logfile. By default, this file is located at `%systemroot%\system32\LogFiles\Firewall\pfirewall.log` and has a maximum size of 4,096 kilobytes.
- Whether to log dropped packets and/or successful connections within the Windows Firewall logfile. By default, neither dropped packets nor successful connections are logged within the Domain, Public, and Private profiles.

#### **NOTE**

---

If you change the location of the Windows Firewall logfile, be sure that the Windows Firewall service account has Write permissions to the new directory.

---

## Modifying IPsec Defaults

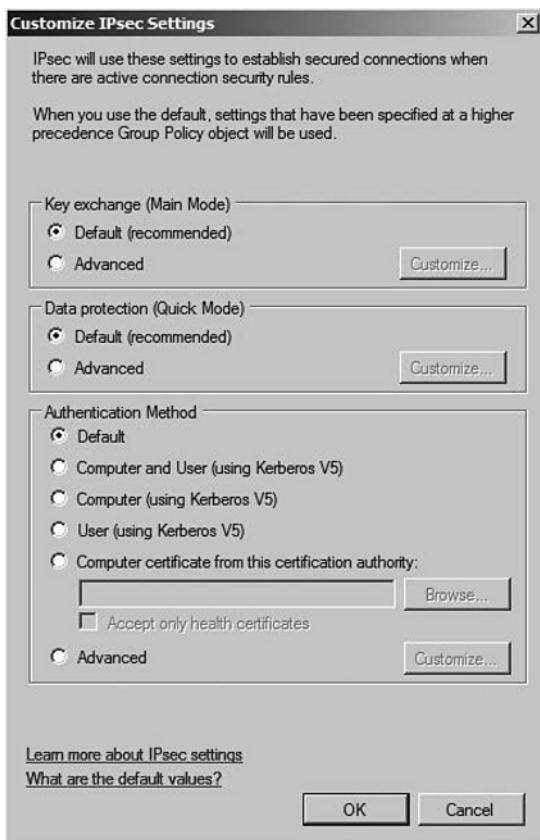
The final tab that you see in Figure 4.17 is the **IPsec Settings** tab; this tab allows you to configure the settings IPsec uses to establish secured connections, as well as whether ICMP traffic should be exempted from IPsec rule processing. These advanced options allow you to configure the default manner in which IPsec handles key exchange, data protection (integrity and encryption), and authentication settings to meet the needs of your network.

**NOTE**

You can still create connection security rules (discussed in the next section) that deviate from these defaults; this simply creates the baseline that all rules will follow unless you specify otherwise.

By default, IPsec exemptions for ICMP are turned off; however, you may want to enable these exemptions to allow for troubleshooting of network connectivity by allowing PING and TRACERT traffic to pass through the Windows Firewall. By clicking **Customize** from the **IPsec Defaults** header, you can customize the default behavior of IPsec from the screen shown in Figure 4.18.

**Figure 4.18** Viewing the Default IPsec Settings



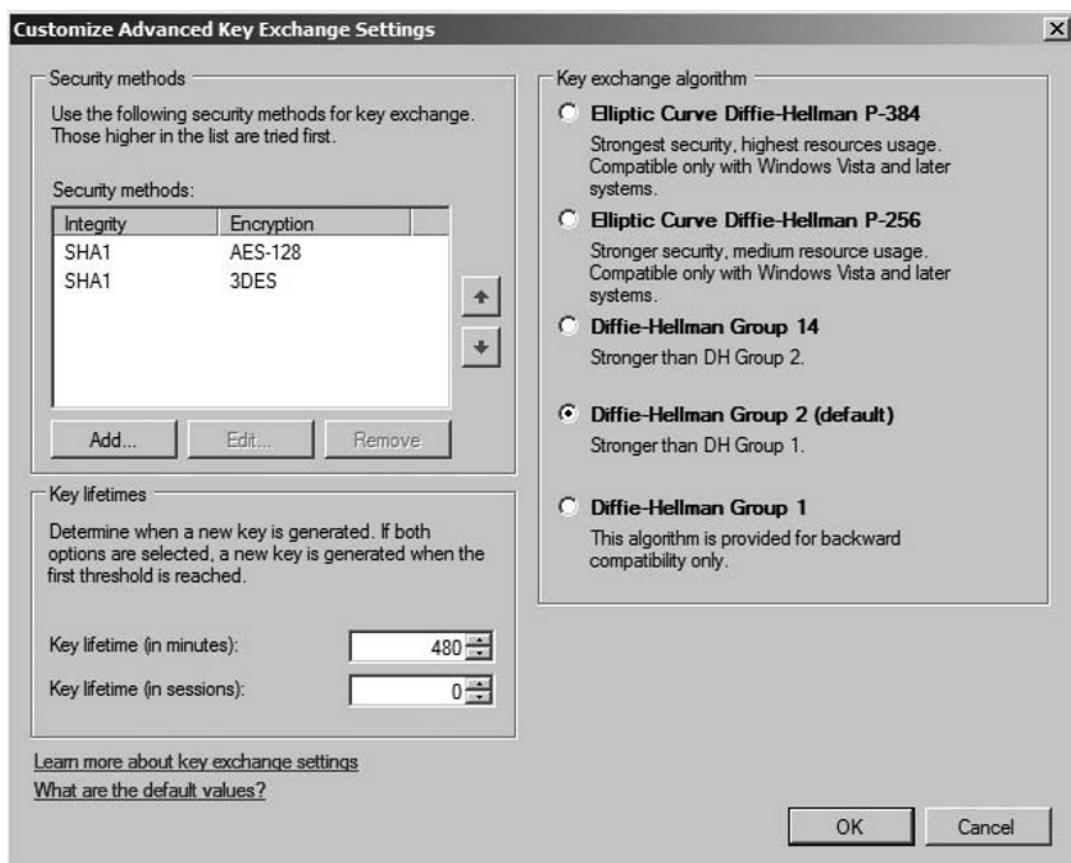
From here, you can customize IPsec's default behavior in several areas, as we discuss in the following sections.

## Key Exchange (Main Mode)

IPsec key exchange is used to establish authentication and data encryption between two computers. This process is divided into two phases: *Main Mode* and *Quick Mode*. In Main Mode, the two computers that are communicating use the IKE protocol to set up a secure, authenticated channel between them. This process creates a Main Mode security association (SA). You'll sometimes also hear this referred to as a *Phase I SA*. The settings that you define here will apply to all IPsec connection security rules that you create (we'll discuss connection security rules next); the default settings that are used to create a Main Mode SA are as follows:

- **Key lifetime (minutes)** 480 minutes.
- **Key lifetime (sessions)** 0. Having a key lifetime of zero sessions forces any new keys to be issued in accordance with the **Key lifetime (minutes)** setting only.
- **Key exchange algorithm** Diffie-Hellman Group 2.
- **Security methods (integrity)** IPsec security methods include both integrity algorithms and encryption algorithms. You can use any combination of these algorithms in order to secure the key exchanges. You can have as many of these combinations as you want, arranged in whatever order you want. These combinations of integrity and encryption algorithms will be attempted in the order that you've specified; the first combination that is supported by both peer computers will be the one that is used. If the computers are not capable of using any of the combinations that you've defined for IPsec, the two computers will not be able to communicate using IPsec. The default security method used for data integrity is SHA-1.
- **Security methods (encryption)** AES-128 is the primary method, and 3-DES (Triple DES) is the secondary method.

Either you can accept the defaults for Main Mode key exchange, or you can select **Customize** to manually specify any of the settings we've described here. Figure 4.19 illustrates the **Properties** screen where you can modify any of these settings.

**Figure 4.19** Customizing Advanced Main Mode Settings

## Data Protection (Quick Mode)

Phase 2 of the IKE process provides for the integrity and/or encryption of the data that's being transmitted between two computers that have established a Main Mode SA. The default settings for IPsec Quick Mode are as follows:

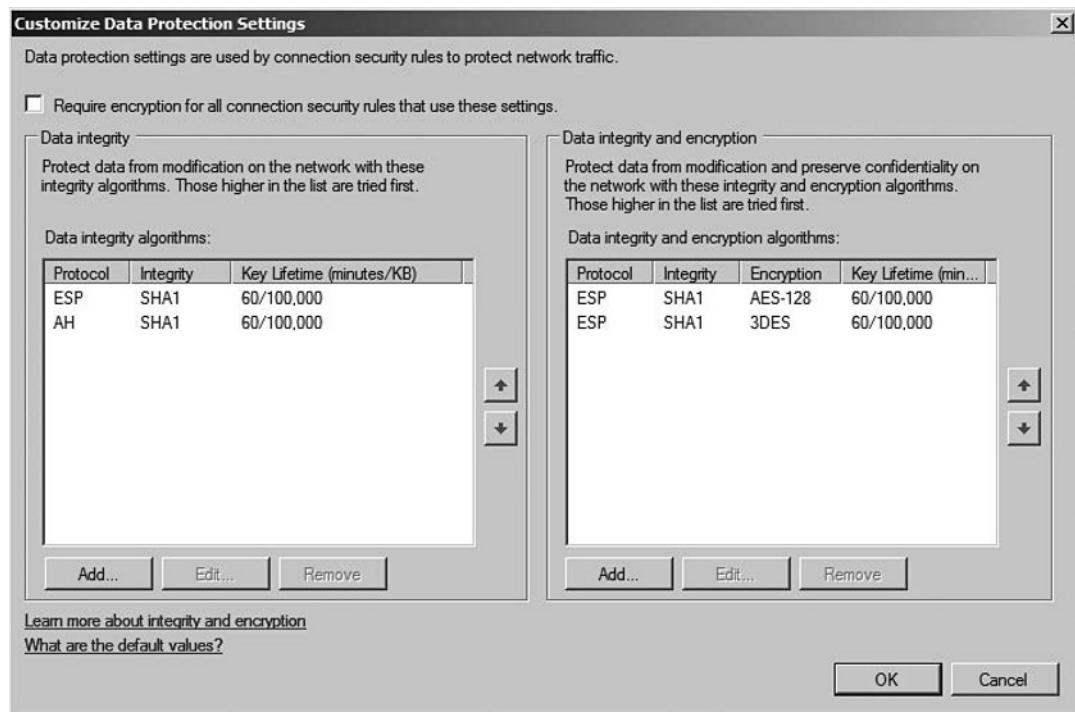
- **Data Integrity** To provide data integrity only within Quick Mode (instead of providing both integrity and encryption), IPsec will first attempt to use the Encapsulating Security Payload (ESP) combined with the SHA-1 data integrity protocol to protect each packet. If ESP protection fails, IPsec will then use the Authentication Header (AH) protocol combined with SHA-1 to protect each packet. When using this method, IPsec does not incorporate any encryption algorithms such as AES or 3-DES.

In both cases, the Quick Mode key lifetime is 60 minutes or 100,000 kilobytes of data transmitted, whichever comes first.

- **Data Integrity and Encryption** To provide for both data integrity and encryption, IPsec will first attempt to communicate using ESP combined with SHA-1 for data integrity and AES-128 for data encryption. If this connection attempt fails, IPsec will attempt to communicate using ESP, SHA-1, and 3-DES encryption. The key lifetime is the same as before: 60 minutes/100,000 KB.

Again, you can either accept the defaults for IPsec Quick Mode, or select **Customize** to manually specify any of the settings we've described here. Figure 4.20 illustrates the **Properties** screen where you can modify any of these settings.

**Figure 4.20** Customizing IPsec Quick Mode Settings



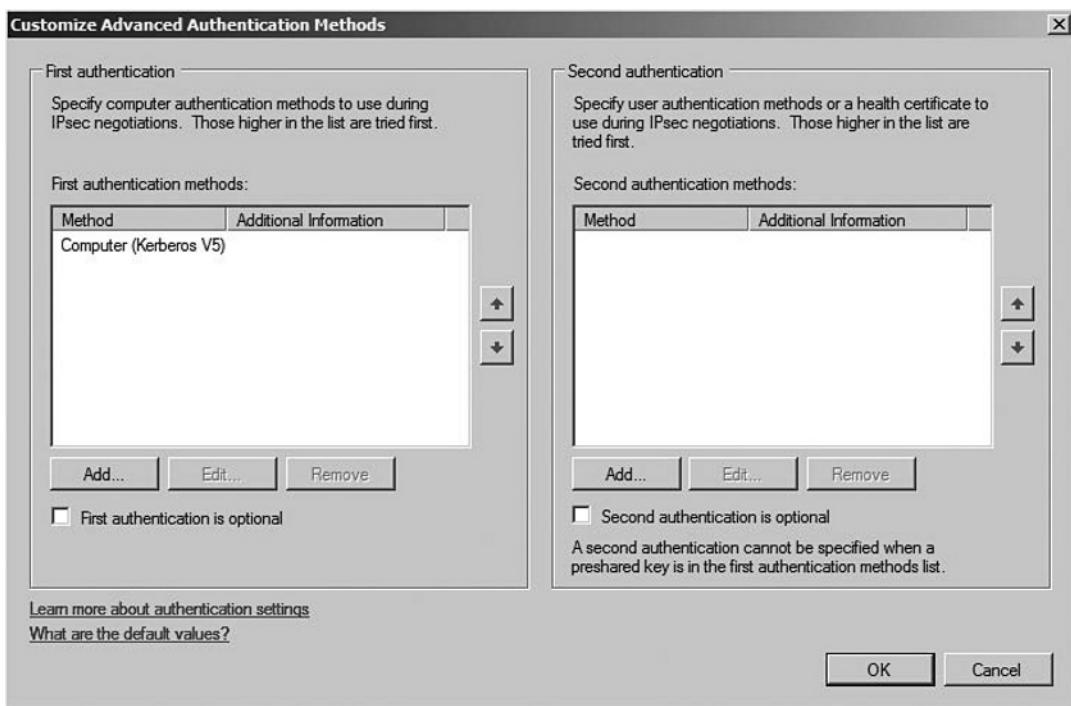
### Authentication Method

The authentication method settings that you select here will determine how two computers will authenticate one another in order to create an IPsec SA. The default

authentication method is Computer (using Kerberos V5), but you can choose any of the following preconfigured methods:

- **Computer and User (using Kerberos V5)** This authentication method requires both computer and user authentication, which means that both the user and the computer must authenticate successfully in order for the two computers to communicate. You can use this option to configure domain isolation, which will create a requirement that any incoming connections to the local computer originate only from domain-joined computer or user objects.
- **Computer (using Kerberos V5)** This method requires only the computer account to authenticate before communication can take place; the computer must be a part of the same Active Directory domain or in a separate domain that has a trust relationship configured. This option creates domain isolation by only allowing incoming connection attempts from domain-joined computers.
- **User (using Kerberos V5)** Similar to the preceding method, this method requires authentication from the user who is logged on to the remote computer; the user must belong to the same Active Directory domain or a trusted domain. This option creates domain isolation by only allowing incoming connections from Active Directory user accounts in the same domain or in a trusted domain.
- **Computer certificate from this certification authority** This method will authenticate computers using certificates issued by a particular certificate authority (CA). This method is useful if you need to allow IPsec traffic to nondomain-joined computers or computers that are members of nontrusted Active Directory domains. You can further specify that this method will accept only health certificates, which the Network Access Protection (NAP) service uses to confirm that a computer that is requesting a connection is up-to-date on patching, antivirus, and other health checks that are required for access to the network.

By clicking on **Advanced | Customize**, you can configure a custom combination of authentication methods; Figure 4.21 illustrates the settings that you can configure in this way.

**Figure 4.21** Creating a Custom Authentication Method

The **First authentication** method describes how the computer account is authenticated, and the **Second authentication** method describes user authentication. As you can see, you can specify that one of these steps is optional; user-only authentication would use **Second authentication** only, for example. When you click **Add** within the **First authentication** section, you see the screen shown in Figure 4.22.

### WARNING

Although it is technically possible to make both First authentication and Second authentication optional, this is not recommended because doing so effectively disables IPsec authentication within your environment.

**Figure 4.22** Customizing Computer Authentication

When creating a custom method for computer authentication, you can select from one of the following options:

- **Computer (Kerberos V5)** This is the default method for First authentication and will authenticate a computer in the same or in a trusted domain using Kerberos V5.
- **Computer (NTLMv2)** This method is used for backward compatibility and to provide authentication for nondomain-joined PCs or PCs joined to untrusted domains.
- **Computer certificate from this certification authority (CA)** This method will authenticate computers using certificates issued by a particular CA. You can further control this method by selecting one or both of the following:

1. **Accept only health certificates** This will accept only certificates that the NAP process utilizes.
  2. **Enable certificate to account mapping** This allows you to map a certificate to one or more computer accounts within Active Directory, thus allowing you to use a single certificate for a group of computers.
- **Preshared key (not recommended)** This is the least secure authentication method and Microsoft does not recommend it; it is present only for backward compatibility and to ensure compliance with the RFC standards for IPsec. If you configure a preshared key as the First authentication method, you cannot use any method for Second authentication.

Figure 4.23 illustrates the options available when creating a custom method for Second authentication. Similar to First authentication, you can create a custom user authentication method by selecting one of the following:

- **User (Kerberos V5)** This is the default method for Second authentication and can authenticate any user in the local domain or in any trusted domain.
- **User (NTMLv2)** This method exists for backward compatibility and to authenticate nondomain-joined users.
- **User certificate from this certification authority (CA)** This method will authenticate users using certificates issued by a particular CA. You have the option to enable certificate-to-account mapping in order to use a single certificate to authenticate one or multiple users.
- **Computer health certificate from this certification authority (CA)** Allows you to authenticate using computer health certificates used by the NAP service. You again have the option to enable certificate-to-account mapping of NAP health certificates.

**Figure 4.23** Customizing User Authentication

## Creating Connection Security Rules

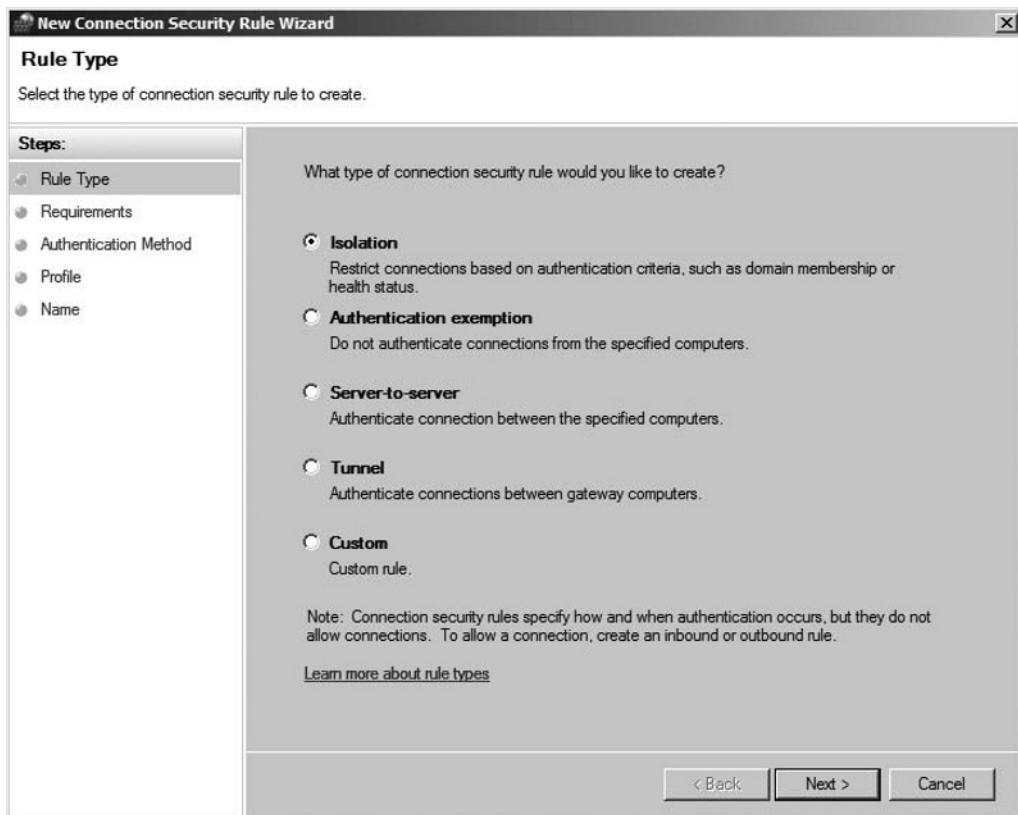
Once you've configured the default IPsec behavior for your individual computer or for an entire network, you can create connection security rules that will define how the Windows Firewall with Advanced Security will enforce authentication requirements for different situations. You can view any existing rules by clicking on **Connection Security Rules** from the main screen of the MMC snap-in. If you right-click on **Connection Security Rules**, you can view only a subset of these rules, filtered in one of two ways:

- **Filter by Profile** will show only those rules that have been configured for the Domain, Private, or Public profile. Selecting **Show All** will remove any filters.
- **Filter by State** will show only those rules that are currently enabled or disabled. Again, selecting **Show All** will remove any filters and display all defined rules.

To create a new rule, right-click on **Connection Security Rules** and select **New Rule**. You'll see the screen shown in Figure 4.24. You can create one of the following types of connection security rules; we will discuss each one in turn:

- An isolation rule will restrict connections to one or more computers based on authentication criteria, by using domain memberships, certificates issued by a CA, or network health certificates issued by NAP.
- An authentication exemption rule will allow a connection to take place without attempting to authenticate the two computers involved.
- A server-to-server connection security rule will authenticate a connection between two specific computers.
- A tunnel connection security rule will authenticate connections between two gateway computers—for example, two computers that are being used to configure a site-to-site VPN.
- A custom connection security rule will allow you to define the exact parameters that the rule should abide by, if one of the preconfigured choices is not appropriate.

**Figure 4.24** Creating a Connection Security Rule



## EXERCISE 4.4

### CONFIGURING AN ISOLATION RULE

1. To configure an isolation connection security rule, select **Isolation** from the screen shown in Figure 4.24 (above) and then click **Next**. You will then be prompted to select one of the following three authentication requirements for the new isolation rule:
  - Request authentication for inbound and outbound connections
  - Require authentication for inbound connections and request authentication for outbound connections
  - Require authentication for inbound and outbound connections
2. Once you have made your choice, click **Next**. You will then be prompted to select the authentication method that this rule should use. Choose among the following:
  - Default
  - Computer and User (Kerberos V5)
  - Computer (Kerberos V5)
  - Computer Certificate. If you select this option, you will be prompted to enter the name of a CA on your network. You will also have the option to accept only NAP health certificates.
  - Advanced. If you select this option, you will be prompted to configure a custom authentication method as described in the “Authentication Method” section, earlier in this chapter.
3. Once you have made your choice, click **Next**. You will then be prompted to select which Windows Firewall profile will apply this rule: Domain, Public, and/or Private. You can configure this rule to be enforced under one, two, three, or none of the Windows Firewall profiles.
4. Click **Next** to continue. You’ll be prompted to enter a name and an optional description for this rule.
5. Click **Finish** when you’re done. You’ll be returned to the main MMC snap-in window, where you will see the newly created rule listed in the main window.

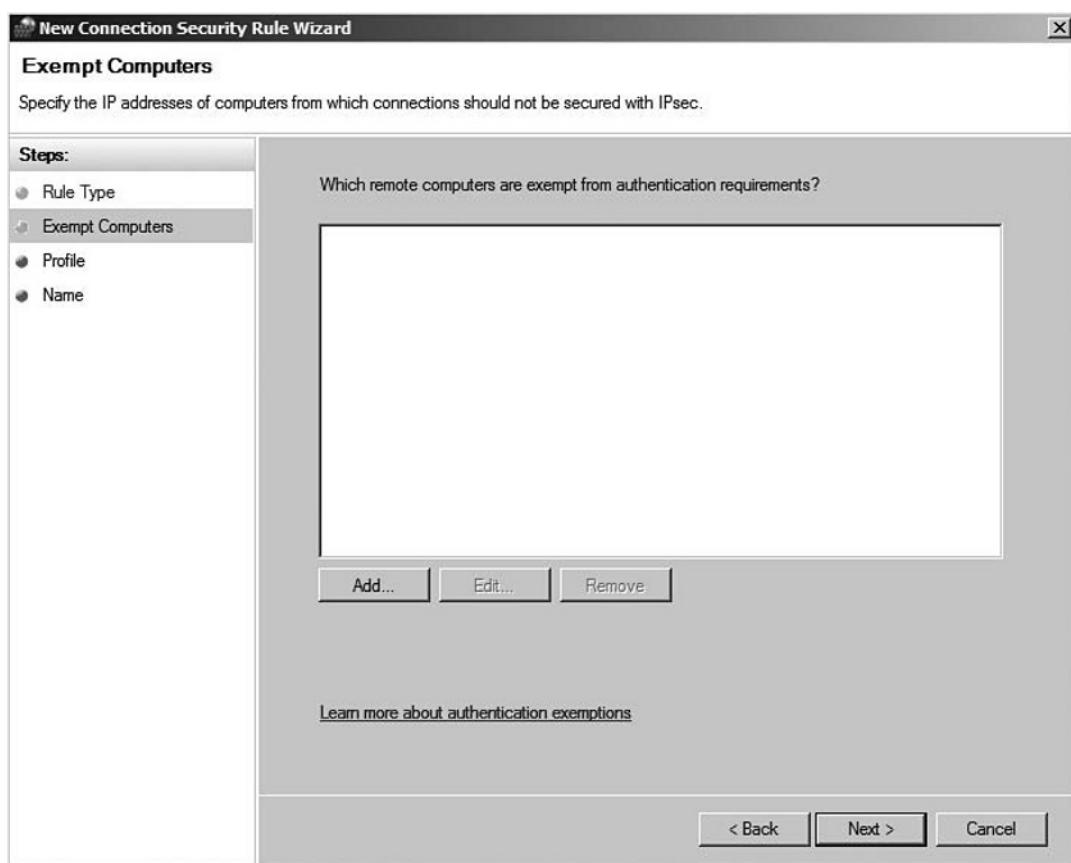
6. From here, you can right-click on the rule to disable or delete it, or you can select **Properties** to modify any of the settings that you configured in the wizard.
- 

## EXERCISE 4.5

### CONFIGURING AN AUTHENTICATION EXEMPTION RULE

1. To create an authentication exemption rule, perhaps for a destination computer that does not support IPsec or that needs to be made available to public-facing clients, select **Authentication Exemption** from the screen shown in Figure 4.24 and click **Next**.
2. Click **Add** to configure the list of computers that should be exempt from IPsec authentication; you'll see the screen shown in Figure 4.25. You can configure exemptions for one or more single IP addresses, for a range of IP addresses, or for one of the following predefined sets of computers:
  - Default gateway
  - Windows Internet Name Service (WINS) servers
  - DHCP servers
  - DNS servers
  - Local subnet. This includes all computers available to the local computer, except for any that are configured with public IP addresses (interfaces). This includes both local area network (LAN) and wireless addresses.

**Figure 4.25** Defining a List of IP Addresses



3. When you've added all of the IP addresses or devices that should be exempt from IPsec authentication, click **Next**.
4. You will then be prompted to select which Windows Firewall profile will apply this rule: Domain, Public, and/or Private. You can configure this rule to be enforced under one, two, three, or none of the Windows Firewall profiles. Click **Next** to continue.
5. You'll be prompted to enter a name and an optional description for this rule. Click **Finish** when you're done.
6. You'll be returned to the main MMC snap-in window, where you will see the newly created rule listed in the main window. From here, you can right-click on the rule to disable or delete it, or you can select **Properties** to modify any of the settings that you configured in the wizard.

## *Configuring a Server-to-Server Connection Security Rule*

To configure a connection security rule that defines how authentication should take place between a specific set of servers or devices, select **Server-to-Server** and click **Next**.

To specify individual devices to which this rule should apply, click **Add**. You'll be taken to the **IP Address** screen where you'll be able to specify one or more single IP addresses, a range of IP addresses, or one of the predefined sets of devices discussed in the "Configuring an Authentication Exemption Rule" section. You can also select **Customize** to specify the type of interface to which the rule should apply: LAN, remote access, or wireless. The rule can be applied to one, two, or all three of these interface types; it will be applied to all interface types by default.

Click **Next** once you have specified the endpoints to which this rule should apply. You will then be prompted to select one of the following three authentication requirements for the new isolation rule:

- Request authentication for inbound and outbound connections
- Require authentication for inbound connections and request authentication for outbound connections
- Require authentication for inbound and outbound connections

Click **Next** once you've made your selection. You can then choose from one of the following three authentication methods:

- **Computer Certificate** If you select this option, you will be prompted to enter the name of a CA on your network. You will also have the option to accept only NAP health certificates.
- **Preshared key** As we discussed earlier, this is a low-security authentication method that Microsoft does not recommend; it is included only for backward compatibility and to ensure compliance with the IPsec RFC standards.
- **Advanced** If you select this option, you will be prompted to configure a custom authentication method as described earlier, in the "Authentication Method" section.

When you've selected the authentication method that this rule should use, click **Next**. You will then be prompted to select which Windows Firewall profile will apply this rule: Domain, Public, and/or Private. You can configure this rule

to be enforced under one, two, three, or none of the Windows Firewall profiles. Click **Next** to continue. You'll be prompted to enter a name and an optional description for this rule. Click **Finish** when you're done. You'll be returned to the main MMC snap-in window, where you will see the newly created rule listed in the main window. From here, you can right-click on the rule to disable or delete it, or you can select **Properties** to modify any of the settings that you configured in the wizard.

## Creating Firewall Rules

In addition to configuring connection security rules, you can use the Windows Firewall with Advanced Security MMC snap-in to exert far more granular control over inbound traffic rules than is available within the Control Panel applet. You can view any existing inbound rules by clicking on **Inbound Rules** from the main screen of the MMC snap-in; likewise, you can view any existing outbound rules by clicking on **Outbound Rules**. If you right-click on either of these nodes, you can view only a subset of these rules, filtered in one of three ways:

- **Filter by Profile** will show only those rules that have been configured for the Domain, Private, or Public profile. Selecting **Show All** will remove any filters.
- **Filter by State** will show only those rules that are currently enabled or disabled. Again, selecting **Show All** will remove any filters and display all defined rules.
- **Filter by Group** will only show rules that are associated with a particular predefined rule set, such as BITS Peercaching or Connect to a Network Projector, or you can display only those rules that are not associated with a group. Selecting **Show All** will remove any filters.

To create a new rule, right-click on **Inbound Rules** and select **New Rule**. You'll see the screen shown in Figure 4.26. You can create one of the following types of inbound rules; we will discuss each one in turn:

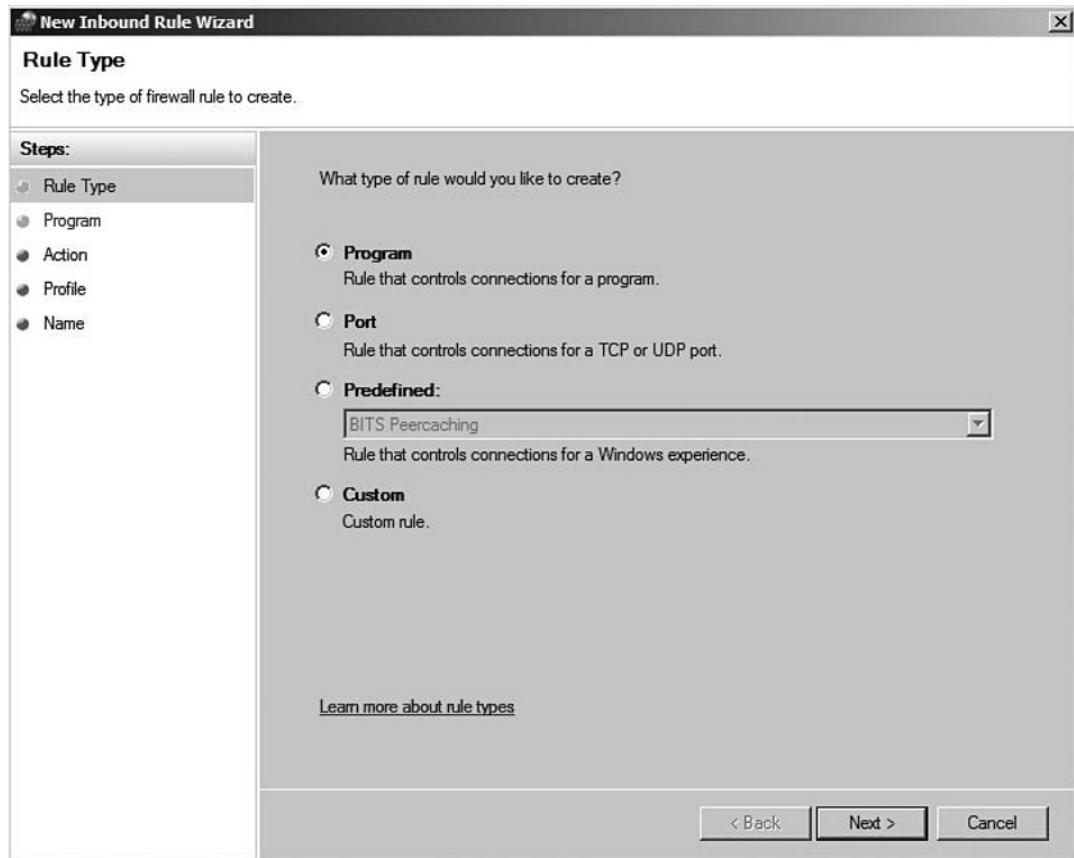
- **Program** creates a rule that is associated with a particular executable file, similar to the **Add Program** option on the **Exceptions** tab of the Windows Firewall Control Panel applet.
- **Port** creates a rule associated with a network port, similar to the **Add Port** option in the Windows Firewall Control Panel applet.

- **Predefined** creates a rule associated with one of the services that have been predefined within the Windows Vista firewall, such as BITS Peercaching or Network Discovery.
- **Custom** creates a custom rule when none of the preconfigured choices is appropriate for your needs.

### NOTE

The GUI screens used in creating an inbound rule and an outbound rule are nearly identical; we will be creating an inbound rule in the following example and we'll point out any differences as needed.

**Figure 4.26** Creating a New Firewall Rule



## EXERCISE 4.6

### CREATING A NEW INBOUND RULE

1. To configure a firewall rule associated with a particular application, select **Program** from the screen shown in Figure 4.26 and click **Next**. You can create a rule that applies to one of the following:
  - **All programs** affects all programs that are installed on the local computer.
  - **This program path** allows you to click **Browse** to select an individual EXE file.
2. Click **Next** when you have made your selection. You'll be prompted to select one of the following **Actions** that should be taken when an executable is found that matches this rule:
  - **Allow the connection.**
  - **Allow the connection if it is secure.** If you select this option, you can select one or both of the following additional options:

**Require the connections to be encrypted.**

**Override block rules.** This enables the Authenticated IPsec Bypass option that will allow IPsec-authenticated users and computers to bypass inbound firewall rules. This option is available only when configuring an inbound rule.
  - **Block the connection.**

#### WARNING

If your Windows Firewall configuration is set to **Block All Connections** (or if you've selected the **Block All Incoming Connections** option from the Control Panel applet), Authenticated IPsec Bypass will have no effect and the incoming traffic in question will still be blocked.

3. Click **Next** once you have chosen the appropriate action for this rule to take. If you select **Allow the connection if it is secure**, you will be taken to a window for restricting by computer or user.

4. To restrict connections to only specific computers, place a checkmark next to **Only allow connections from these computers**; click **Add** to add one or more Active Directory computer accounts to the firewall rule.
5. To restrict inbound connections to specific Active Directory user objects, place a checkmark next to **Only allow connections from these users**; click **Add** to specify one or more Active Directory user or group objects. Both of these checkboxes are optional; you do not need to restrict the rule to specific users or computers if you do not want to do so.



### NOTE

When creating an outbound rule, the wizard will read **Only allow connections to these computers**. In addition, the option to restrict connections according to user accounts will not be available.

6. If you were taken to the **Users and Computers** screen click **Next** once you have made the appropriate selections. Once you have made your choice, click **Next**.
7. You will then be prompted to select which Windows Firewall profile will apply this rule: Domain, Public, and/or Private. You can configure this rule to be enforced under one, two, three, or none of the Windows Firewall profiles. Click **Next** to continue.
8. You'll be prompted to enter a name and an optional description for this rule. Click **Finish** when you're done.
9. You'll be returned to the main MMC snap-in window, where you will see the newly created rule listed in the main window. From here, you can right-click on the rule to disable or delete it, or you can select **Properties** to modify any of the settings that you configured in the wizard.

## Configuring & Implementing...

### Configuring the Windows Firewall from the Command Line

In addition to the GUI configuration options we've outlined thus far, you can also administer the Windows Firewall using the *netsh* command-line utility. *Netsh* allows you to configure and monitor the Windows Firewall by creating rules, monitoring connections, and displaying the status of the Windows Firewall.

To access *netsh* simply go to the command prompt and enter **netsh advfirewall**. From this context, you will have the following subcommands available:

- **export** Exports the current firewall policy to a file.
- **help** Displays a list of available commands.
- **import** Imports the firewall configuration from a particular file.
- **reset** Restores the Windows Firewall to its default configuration.
- **set file** Copies the console output to a file.
- **set machine** Denotes the computer that should be configured.
- **show allprofiles** Displays the firewall properties for all three profiles.
- **show domainprofile** Displays the firewall properties for the domain profile.
- **show privateprofile** Displays the firewall properties for the private profile.
- **show publicprofile** Displays the firewall properties for the public profile.

You can also access the following additional subcontexts to configure additional aspects of the Windows Firewall:

Continued

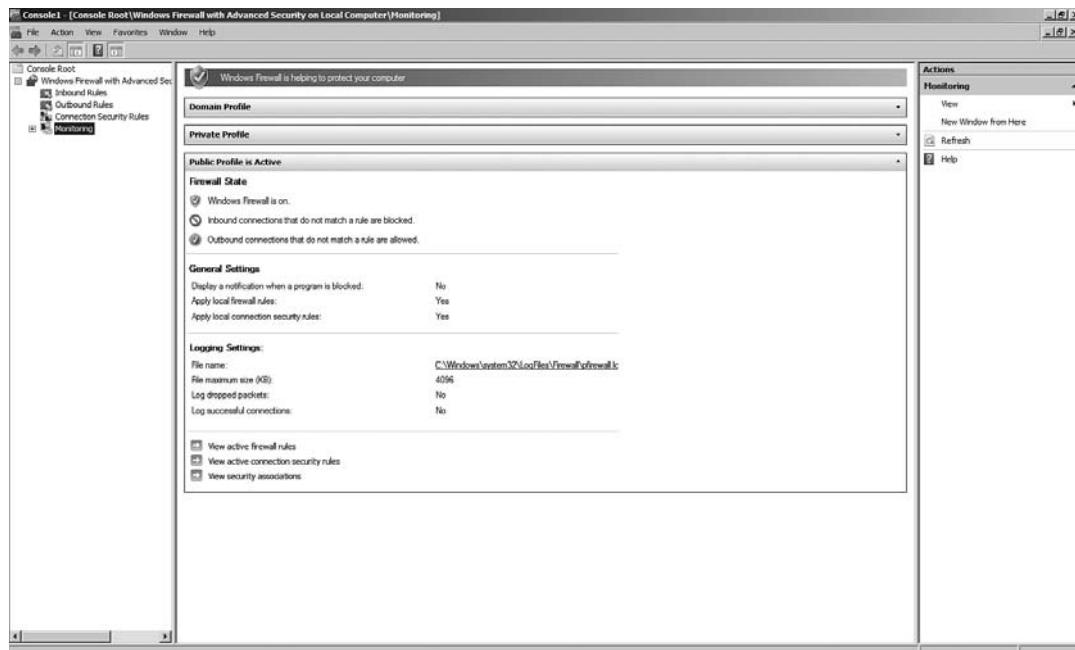
- **consec** View and configure connection security rules.
- **inbound** View and configure inbound firewall rules.
- **outbound** View and configure outbound firewall rules.
- **monitor** View and configure monitoring information.

And of course, you can obtain help from any *netsh* menu by simply typing **?** and pressing **Enter**.

## Monitoring the Windows Firewall

Using the Windows Firewall with Advanced Security MMC snap-in, administrators now have access to real-time firewall configuration information that can be invaluable in troubleshooting connectivity issues on Windows Server 2008. Simply open the MMC snap-in and select **Monitoring** in the left-hand pane, as shown in Figure 4.27.

**Figure 4.27** Monitoring the Windows Firewall

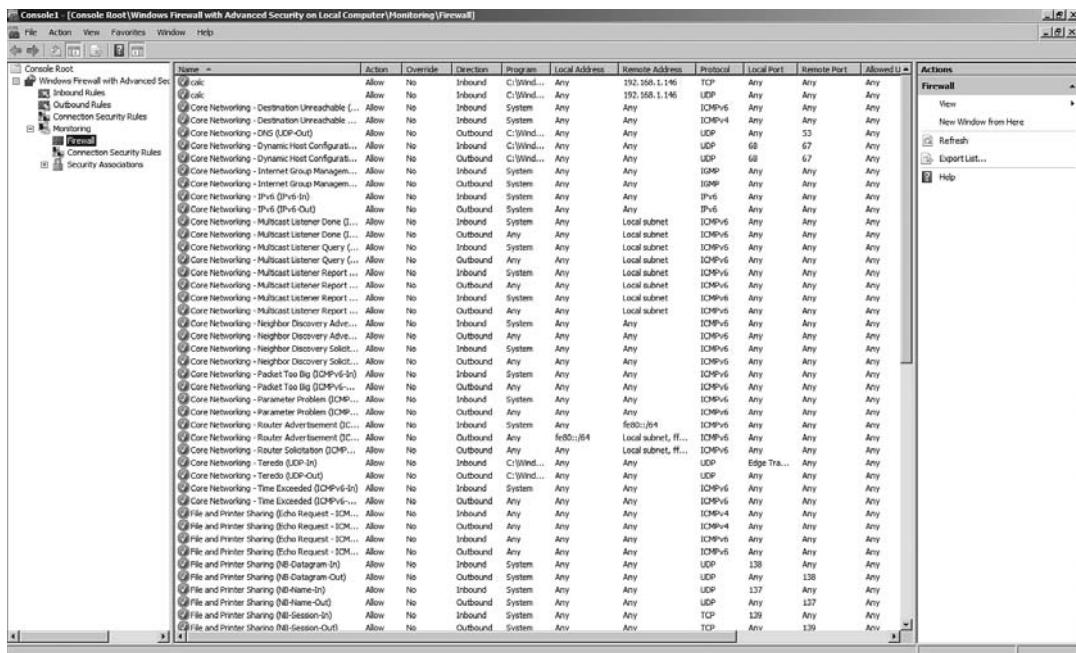


From the main **Monitoring** screen shown in Figure 6.37, you will see an at-a-glance summary of your current firewall settings, describing the overall state of the firewall, which profile is active, as well as notification and logging settings. You also have the ability to drill down to a detailed view of any of the following:

- Active firewall rules
- Active security connection rules
- Active IPsec SAs

In Figure 4.28, you can see the information that is displayed when you drill down to the Firewall node: which firewall rules are currently active, and specific details on each rule including the name of the rule, the action associated with that rule (allow, secure, block), whether it is an inbound or outbound firewall rule, and much more.

**Figure 4.28** Monitoring Active Firewall Rules



The screenshot shows the Windows Firewall with Advanced Security Monitoring interface. The left pane displays a tree view of security profiles: Console Root, Windows Firewall with Advanced Security, Inbound Rules, Outbound Rules, Connection Security Rules, Firewall, and Security Associations. The Firewall node is selected. The right pane shows a detailed list of active firewall rules. The columns include Name, Action, Override, Direction, Program, Local Address, Remote Address, Protocol, Local Port, Remote Port, and Allowed U. A context menu is open over the list, with options like View, New Window from Here, Refresh, Exportlist..., and Help.

Name	Action	Override	Direction	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Allowed U
calc	Allow	No	Inbound	C:\Wind...	Any	192.168.1.146	TCP	Any	Any	Any
calc	Allow	No	Inbound	C:\Wind...	Any	192.168.1.146	UDP	Any	Any	Any
Core Networking - Destination Unreachable (...	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Destination Unreachable (...	Allow	No	Inbound	System	Any	Any	ICMPv4	Any	Any	Any
Core Networking - DNS (UDP-In)	Allow	No	Outbound	C:\Wind...	Any	Any	UDP	Any	53	Any
Core Networking - Dynamic Host Configuration...	Allow	No	Inbound	C:\Wind...	Any	Any	UDP	68	67	Any
Core Networking - Dynamic Host Configuration...	Allow	No	Outbound	C:\Wind...	Any	Any	UDP	67	68	Any
Core Networking - Internet Group Managem...	Allow	No	Inbound	System	Any	Any	ICMP	Any	Any	Any
Core Networking - Internet Group Managem...	Allow	No	Outbound	System	Any	Any	ICMP	Any	Any	Any
Core Networking - IPv6 (In-)	Allow	No	Inbound	System	Any	Any	IPv6	Any	Any	Any
Core Networking - IPv6 (In-)	Allow	No	Outbound	System	Any	Any	IPv6	Any	Any	Any
Core Networking - Multicast Listener Done (...	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Done (...	Allow	No	Outbound	Any	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Query (...	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Query (...	Allow	No	Outbound	Any	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report (...	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report (...	Allow	No	Outbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report (...	Allow	No	Inbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Multicast Listener Report (...	Allow	No	Outbound	System	Any	Local subnet	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Adve...	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Adve...	Allow	No	Outbound	Any	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Solict...	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Neighbor Discovery Solict...	Allow	No	Outbound	Any	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Packet Too Big (ICMPv4-3)	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Packet Too Big (ICMPv4-3)	Allow	No	Outbound	Any	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Parameter Problem (ICMP...	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Parameter Problem (ICMP...	Allow	No	Outbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Router Advertisement (IC...	Allow	No	Inbound	System	Any	fe80::1%4	ICMPv6	Any	Any	Any
Core Networking - Router Advertisement (IC...	Allow	No	Outbound	Any	fe80::1%4	Local subnet, ff...	ICMPv6	Any	Any	Any
Core Networking - Router Solicitation (IC...	Allow	No	Inbound	Any	Any	Local subnet, ff...	ICMPv6	Any	Any	Any
Core Networking - Router Solicitation (IC...	Allow	No	Outbound	C:\Wind...	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Teredo (UDP-In)	Allow	No	Inbound	C:\Wind...	Any	Any	UDP	Edge Tra...	Any	Any
Core Networking - Teredo (UDP-Out)	Allow	No	Outbound	C:\Wind...	Any	Any	UDP	Any	Any	Any
Core Networking - Time Exceeded (ICMPv6-5)	Allow	No	Inbound	System	Any	Any	ICMPv6	Any	Any	Any
Core Networking - Time Exceeded (ICMPv6-5)	Allow	No	Outbound	Any	Any	Any	ICMPv6	Any	Any	Any
File and Printer Sharing (Echo Request - ICM...	Allow	No	Inbound	Any	Any	Any	ICMPv4	Any	Any	Any
File and Printer Sharing (Echo Request - ICM...	Allow	No	Outbound	Any	Any	Any	ICMPv4	Any	Any	Any
File and Printer Sharing (ECHO Request - ICM...	Allow	No	Inbound	Any	Any	Any	ICMPv6	Any	Any	Any
File and Printer Sharing (ECHO Request - ICM...	Allow	No	Outbound	Any	Any	Any	ICMPv6	Any	Any	Any
File and Printer Sharing (NB-Catagram In)	Allow	No	Inbound	System	Any	Any	UDP	138	Any	Any
File and Printer Sharing (NB-Catagram In)	Allow	No	Outbound	System	Any	Any	UDP	138	Any	Any
File and Printer Sharing (NB-Name-In)	Allow	No	Inbound	System	Any	Any	UDP	137	Any	Any
File and Printer Sharing (NB-Name-Out)	Allow	No	Outbound	System	Any	Any	UDP	137	Any	Any
File and Printer Sharing (NB-Session-In)	Allow	No	Inbound	System	Any	Any	TCP	139	Any	Any
File and Printer Sharing (NB-Session-In)	Allow	No	Outbound	System	Any	Any	TCP	139	Any	Any

## Data Security

Regardless of if you are working with servers or workstations, it is important to ensure that the data on the computer is protected whether it is in an active or saved

(inactive) state. What this means is, we need to be able to protect our data when a system is powered on and the operating system is running, or if the machine is booted into an alternate operating system, or there has been a change in hardware configuration—a hard drive being placed into another system, for example. Windows Server 2008 provides security features for both of these solutions.

Everyone has heard the new reports about laptops being stolen, temporarily misplaced, or lost. The data stored on the hard drive can be retrieved by means other than through the operating system. Things like bootable CDs or USB keys can be used to bypass the operating system and get directly to the information stored on the physical media without the need to know any passwords. Once the operating system has been bypassed, all the files on the drive can be viewed, edited, or copied. The best safeguard to defend against this security issue is encryption.

BitLocker is Microsoft's answer to providing better security by encrypting the data stored on the operating system volume of the drive and is only available in the Windows Server 2008 or the Enterprise and Ultimate versions of Vista. This new security feature goes a long way to help users and organizations protect their data.

Encrypted File System (EFS) has a much longer legacy than BitLocker, and is a proven solution for protecting the integrity of documents. With EFS, we have the ability to encrypt either individual files or entire folders, guaranteeing the security of the document, and preventing them from being accessed by unauthorized users.

Let's begin our discussing of Data Security with an overview of the BitLocker tool.

## BitLocker

Windows Server 2008, along with the Enterprise and Ultimate editions of Windows Vista, includes a new technology from Microsoft known as BitLocker that will encrypt a data volume. As of the time of this writing, there is no known back door for hackers or law enforcement. BitLocker is a technology from Microsoft that will encrypt an entire volume. Forensic Software Tools like EnCase, FTK, or X-Ways Forensics will not be able to read data from BitLocker encrypted drives.

BitLocker can be implemented with or without a TPM chip on Windows Server 2008 or Windows Vista. A TPM, or Trusted Platform Module, as seen in Figure 4.29, is a unique chip on the motherboard that will store keys, passwords, and certificates. The TPM chip will check to make sure that hardware and software in the machine has not been altered. If a hard drive is pulled out of a machine that is using BitLocker in conjunction with a TPM chip, that hard drive will be unreadable. The TPM chip needs to be initialized in the BIOS; while using the TPM chip will add security to a system, the configuration of BitLocker with a TPM will be a bit more difficult.

**TEST DAY TIP**

Know that if you are planning to use a TPM in conjunction with BitLocker, it must be TPM 1.2 or higher.

**Figure 4.29** Trusted Platform Module

**EXAM WARNING**

A TPM Chip is not required to use BitLocker on a system running the Windows Server 2008, Vista Ultimate, or Enterprise Edition. Settings can be adjusted through Group Policy to allow a computer without a TPM to utilize BitLocker.

Setting up BitLocker on a system that already has Windows Server 2008 is a relatively easy process. Before reconfiguring the partitions on your system, it is imperative that you backup your data. USB Mass storage devices with 200 MB of storage can be purchased for less than 100 dollars. When a system is repartitioned, performing a backup is always a good idea because there is a chance that something might go wrong and your data could be lost.

**EXAM WARNING**

BitLocker, available only on the Ultimate and Enterprise Editions of Vista, requires more than one partition on a disk. A separate boot partition of at least 1.5 MB is required. This partition will have some unencrypted information. The system volume partition will be fully encrypted.

As mentioned, BitLocker can still be loaded on a system without a TPM; however, it can not be utilized on a system that has not been properly partitioned. A partition is a logical division of a disk; even though you may have only one physical disk, you can have up to four partitions on that disk (for disks using MBR, not GPT). For disks that only have a single partition or are not partitioned properly for BitLocker, the BitLocker Drive Preparation tool can be used.

## Encrypted File System

The encrypted file system has been around since Windows 2000. With the initial release of EFS, users could encrypt files or folders. The Encrypted file system, or EFS, would best be utilized on a system not utilizing BitLocker. To encrypt a file, simply right-click on the file, go to **properties**, and select **advanced**. Check the box that says encrypt data to secure contents, as seen in Figure 4.30. By default, encrypted files and folders will be displayed with a green color in Windows.

**Figure 4.30** Using the Encrypted File System



A folder can also be encrypted. When you encrypt a folder, you will be asked if you want to apply the encryption to the folder only or to the folder, all of the subfolders, and files within the folder. Applying the encryption to the folder, all of the subfolders, and files within the folder is recommended. Once this setting is applied, files or folders put into that encrypted folder will also become encrypted.

If you have a preference for using the command line, the cipher command can be utilized to encrypt files and folders, as well as display files and folders with the encryption attribute. There are actually a number of advanced operations that can be performed with the cipher command, as seen in the following example:

```
CIPHER [/E | /D | /C] [/S:directory]
        [/B] [/H] [pathname [...]]
CIPHER /K
CIPHER /R:filename [/SMARTCARD]
CIPHER /U [/N]
CIPHER /W:directory
CIPHER /X[:efsfile] [filename]
CIPHER /Y
CIPHER /ADDUSER [/CERTHASH:hash | /CERTFILE:filename]
        [/S:directory] [/B] [/H] [pathname [...]]
CIPHER /REMOVEUSER /CERTHASH:hash
        [/S:directory] [/B] [/H] [pathname [...]]
```



### TEST DAY TIP

Know the cipher command and the some of the switches that can be used. These enhancements are part of Windows Ultimate extras.

## Auditing

As regulatory bodies such as Sarbanes-Oxley (also commonly known as SARBOX or SOX) and the Health Information Portability and Privacy Act (HIPPA) begin enforcing security regulations on businesses (and other organizations), the need for extensive auditing capabilities continues to grow exponentially. IT organizations are now required to capture a greater depth of information about their environment, as well as retaining this information for a longer period of time.

While improving the auditing capabilities in Windows Server 2008, Microsoft has also revamped the events engine to make it much more flexible and user friendly. We will discuss this later. Understanding how auditing works is crucial—not only for purposes of passing this exam, but also in how you control your Windows-based environment. We will begin our discussing with auditing Directory Services.

## Auditing AD DS and LDS

One of the most significant changes from Windows Server 2003 to Windows Server 2008 in terms of auditing is the ability to now track the changes that were made to attributes of a Directory Services object. With Windows Server 2003, you could very easily turn on auditing, but your audit information was limited to the knowledge that a particular attribute had been changed and who changed it. While this is helpful in terms of tracking when changes are made, it doesn't provide the necessary information to track *what* was changed to the object. This was known as the **Audit directory service access** policy.

With Windows Server 2008, Microsoft has expanded on this policy by introducing four new subcategories of this policy:

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

As mentioned earlier, we can now track changes made to an individual object within Active Directory. For example, if the office telephone number of a user was changed from **978-555-1212** to **617-555-1212**, we now have the ability to create a record within our event logs which will show what record was changed, who changed it, and what was changed. Directory Services Replication and Detailed Replication are fairly self-explanatory. These subcategories allow for very high-level replication information between domain controllers (both inter- and intra-site replication), as well as a much more detailed replication history. The Detailed Replication history is very useful in situations where you may experiencing inconsistencies, latency, or corruption during the replication of directory services.

### EXERCISE 4.7

---

#### TRACKING DIRECTORY SERVICES CHANGES

1. Click **Start | Administrative Tools | Group Policy Management**.
2. Double-click on your forest.
3. Double-click **Domains** and then double-click the name of your domain.

4. Double-click on **Domain Controllers**, and then right-click **Default Domain Controllers Policy | Edit**.
5. Under Computer Configuration, double-click **Policies**.
6. Next, you need to double-click on **Windows Settings | Security Settings | Local Policies** and finally **Audit Policy**.
7. In Audit Policy, right-click on **Audit directory service access**, and select **Properties**.
8. Click on the **Define these policy settings** check box.
9. Under **Audit these attempts**, select **Success**, and click **OK**.

Now that we have activated the audit policy, we still need to go back and enable auditing on our objects. This is done through the System Access Control List (SACL). What we will now do is create an Access Control Entry (ACE) into our SACL. Without this ACE, in our example above, we would have no way of tracking the phone number change.



### TEST DAY TIP

---

Make sure that answers to any questions relating to DS auditing and tracking directory services changes makes mention of the SACL or it will be incorrect!

---

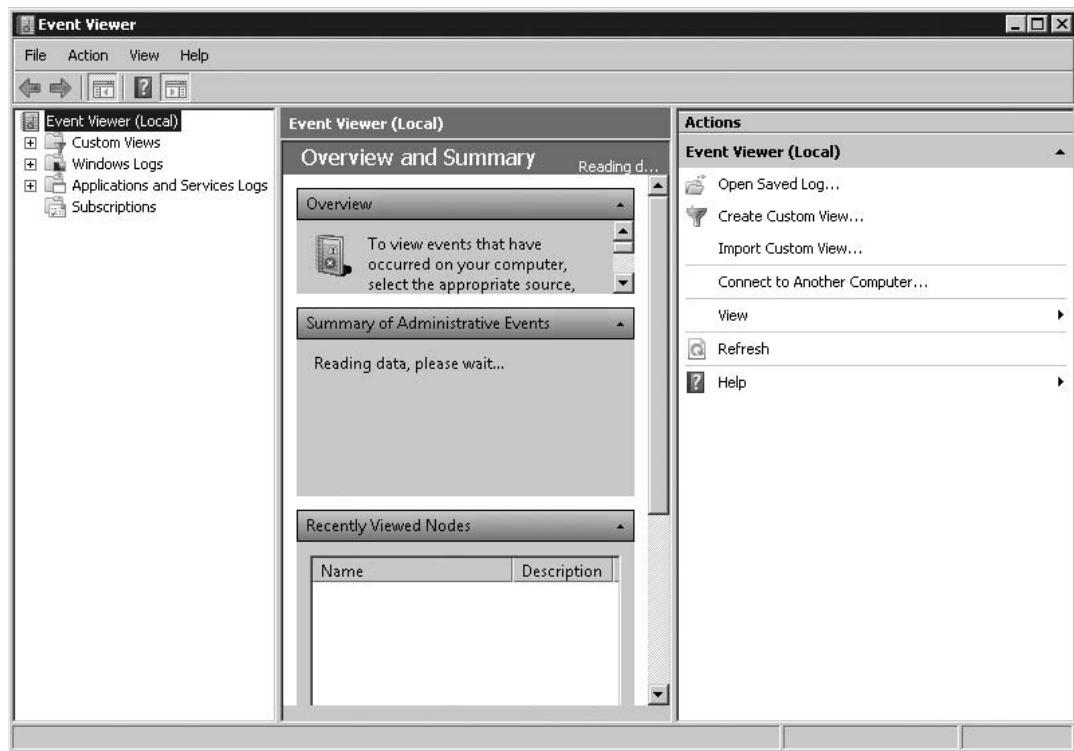
10. Click **Start | Administrative Tools | Active Directory Users and Computers**.
11. Right-click either your domain or an organizational unit which contains objects you want to audit, and then click **Properties**.
12. Click on the **Security** tab, and then click **Advanced**.
13. Next, move to the **Auditing** tab and click **Add**.
14. Under **Enter the object name to select**, type **Authenticated Users**, and then click on **OK**.
15. In **Apply onto**, click **Descendant User objects**.
16. Under **Access**, select the **Successful** check box next to **Write all properties**.

17. Close any open windows.
  18. Finally, try creating, modifying, and moving an object within Active Directory and view the resulting event log records.
- 

## Event Log

With the introduction of Windows Server 2008, Microsoft has introduced the new Windows Eventing 6.0 subsystem. Perhaps one of the most noticeable changes is the redesigned user interface, which includes new features such as customizable views, overview, and summary pages. At the same time, the Explain text has been greatly enhanced to provide much more information about individual events (Figure 4.31).

**Figure 4.31** Revised Event Log UI



While the UI is nice to look at, it is by far the least impressive part of the new Event Log subsystem. One of the more exciting and useful tools is the ability to create “actions” off of individual events. For example, if a change was made to a particular OU (user object, file, etc.), an e-mail can be sent to a particular individual (or group of individuals) to notify them of these changes. Another exciting change with Event Viewer is the ability to control exactly what events are being captured in the event log through a new technology known as Granular Audit Policy (GAP). GAP gives you the ability to break down the pre-existing nine event “categories” into 50 subcategories, allowing you to filter on things such as Files Shares and Registry edits.

### EXAM NOTE

GAP is not configurable through the Group Policy management tool, and can only be managed through the command line. For more information on how to manage GAP, visit <http://support.microsoft.com/kb/921469>.

One of the other major advances in Windows Server 2008 Eventing is Event Subscriptions. Event Subscriptions allow you to forward events from one server to another for purposes of consolidation and coordination. Event Subscriptions are supported by both Windows Server 2008 and Windows Vista, so that events from both servers and clients can be collected in a single location. Event collection is a new service—known as the Windows Event Collector service—that makes this subscription service possible. Configuration of the event hosts (the originator of the event) is fairly simple, and can be added to login scripts for automatic setup of the service through the use of the **winrm** configuration utility.

## Summary of Exam Objectives

In this chapter, we have discussed a number of different topics, spanning from remote access and server security, all the way down to how we manage individual security events on an object. The common theme within the chapter is the focus on the major investments that Microsoft has made into making a Windows-based environment much more secure, while still providing administrators and other IT professionals the ability to manage these new functions through a user-friendly set of tools and wizards.

Starting with the Network Policy and Access Service (NPAS) role, we discussed how many of the disjoined security solutions in Windows Server 2003 had been collected into a single role solution in Windows Server 2008. NPAS provides a centralized solution for management and control of VPN and dial-up access, as well as much more advanced remote access security solutions such as Network Access Protection (NAP). Although Microsoft has made great strides in making many of their product offerings “VPN-less,” there are still many mission-critical applications that require VPN access to internal resources. The introduction of NAP provides IT pros with a tool to better secure their environment through health policy requirements, validation, and remediation.

With server security, Microsoft has expanded on the capabilities of the previous host-based firewall solution, providing for much more granular management of the firewall through the introduction of the Windows Firewall with Advanced Security MMC. Now, IT pros have the ability to not only manage the type of IP traffic allowed to their systems, but they can also manage who and which machines are allowed to connect, along with a much more intuitive solution for IP Security (IPsec) communications. Outside of how Windows handles IP communication to and from the server, they have also introduced the BitLocker technology to Windows Server 2008, thereby protecting information while a server is at rest (offline) and continues to support the Encrypted File System (EFS) technology to protect data while a system is online.

Finally, we discussed how Microsoft improved on both the auditing and event log management in Windows Server 2008. The advances made in the type of data we collect in an event and how it is presented (and escalated) in Windows Server 2008 makes auditing and overall management of user security much more tolerable.

# Exam Objectives Fast Track

## Remote Access Security

- The Network Policy and Access Service (NPAS) is ultimately a role that consists of a number of services: Network Policy Server (NPS), Routing and Remote Access (RRAS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP).
- RRAS supports three Virtual Private Network (VPN) protocols: PPTP, L2TP, and SSTP.
- NAP Health Policies are a combination of settings for health determination and enforcement of infrastructure compliance.
- The following sets of settings make up NAP Health Policies: Connection Request Policies, Network Policies, Health Policies and NAP Settings.
- NAP Health Policies are configured using the Network Policy Server console.
- NPS in Windows 2008 Server replaces IAS in Windows 2003 Server.
- The NAP platform main objective is to validate the state of a client computer before connecting to the private network and offer a source of remediation.
- To validate access to a network based on system health, NAP provides the four areas of functionality: Health state validation, Network access limitation, Automatic remediation, and Ongoing compliance. The three distinct networks are: secure network, boundary network, and restricted network.
- Flexible Host Isolation refers to the ease of network isolation provided with the IPsec method of NAP enforcement.

## Server Security

- The functions that were formerly found on the Advanced tab, as well as a number of new features in the Windows Server 2008 firewall, have been moved to the Windows Firewall with Advanced Security MMC snap-in.
- The Windows Server 2008 firewall allows you to create different firewall settings for the following profiles: domain profile, private profile, and public profile.

- From the main Monitoring screen of the Windows Firewall with Advanced Security MMC, you can see an at-a-glance summary of your current firewall settings, describing the overall state of the firewall, which profile is active, as well as notification and logging settings. You also have the ability to drill down to a detailed view of Active firewall rules, active security connection rules, and Active IPsec SAs.
- While BitLocker does not require a TPM chip to function, it is the recommended method for key storage.

## Auditing

- Windows Server 2008 introduces four new auditing subcategories: Directory Service Access, Directory Service Changes, Directory Services Replication, and Detailed Directory Service Replication.
- It is important to remember that even if the Directory Service Changes subcategory is activated in group policy, it will not report on changes until an ACE is active in a SACL.
- Event Viewer 6.0 provides for a new solution known as event subscriptions, allowing for collection and management of events from both Windows Server 2008 and Windows Vista sources.

# Exam Objectives

## Frequently Asked Questions

**Q:** Is there a difference between BitLocker in Windows Server 2008 and Windows Vista?

**A:** No, the technology is exactly the same between both operating systems.

**Q:** I have set advanced firewall policies for a particular server, and I want to be able to move them to additional servers without recreating them. Is this possible?

**A:** Yes, you can export firewall policies and import them into another system.

**Q:** Is Windows Vista the only client operating system that will support Network Access Protection?

**A:** No, Windows XP (with Service Pack 3) will support it. Third-party companies are also developing NAP clients for Mac OS as well as certain flavors of Linux.

**Q:** I am trying to create an SSTP VPN connection from my Windows Vista PC to a Windows Server 2008 server. However, I do not see an option for SSTP. Am I doing something wrong?

**A:** No, but you need to verify that the Vista system you are using currently has Service Pack 1 (or later) installed.

**Q:** Which version of a Trusted Platform Module chip works with BitLocker?

**A:** TPM Version 1.2

**Q:** What is the digital locker?

**A:** Microsoft offers a Secure Online Key Backup which allows users to store their BitLocker and EFS Recover Keys.

**Q:** I have worked with Windows 2003 Server Network Access Quarantine Control extensively. Will this help me better work with Network Access Protection?

**A:** The short answer is no. Microsoft has totally changed the way network access is controlled in Windows Server 2008. For instance, there is no longer an Internet Authentication Service and Routing and Remote Access Service—these have been wrapped up into the Network Access Protection.

**Q:** You mentioned VLANs in this chapter. I am not very familiar with this technology. Should I seek other sources to help me understand this new subject?

**A:** Definitely! Microsoft probably does not give VLAN technology the time it deserves in its courseware or exams. In the workplace, it is almost a must to understand how VLANs work—especially if you are wanting to work (or already do work) in an enterprise environment. Earlier in this chapter, I gave you a link to a Cisco article that explains VLANs in detail. It would probably be a good idea to go out and give this article a once over.

**Q:** My employer has not installed or migrated to Windows Server 2008 yet. Should I get hands on experience before sitting this exam?

**A:** Yes! The best advice for any Microsoft exam is to actually sit down and work with the product. Go out and download the free copy of Microsoft Virtual PC 2007 and register for a 180 day trial of Windows Server 2008 Enterprise Edition. With Microsoft Virtual PC 2007, you can use multiple virtual machines to build virtual networks. This way you can set up just about any scenario in a test environment.

**Q:** I noticed in this chapter a lot of new acronyms that I never had heard before. This kind of makes me nervous. Is there a way to cover them all?

**A:** There are a lot of new services and server roles with Windows 2008 Server. The best way to learn new acronyms and their meanings are good old fashioned flash cards. Also, keeping a list with any new terms and definitions is always a good study habit.

**Q:** What is the technology in this material that hangs up students the most?

**A:** The technology that seems to always get a lot of questions usually deals with IP Security enforcement and 802.1x. IP Security normally causes students' problems with Certificate Authorities and learning how to manage certificates. There are a lot of good whitepapers on Microsoft TechNet Web site to help you with this topic. Also, 802.1x causes some issues because the student does not understand VLANs and RADIUS. It gets a lot of attention on tests and courseware—but a lot of students have never really got to play with this type of technology.

## Self Test

1. You want to set up a Routing and Remote Access Server using Windows Server 2008. Which of the following protocols are supported in Windows Server 2008?
  - A. PPP
  - B. L2TP
  - C. PPTP
  - D. SSTP
2. You want to enable a Windows Server 2008 system to function as a Router between two networks. Which Role Service of the Network Policy and Access Services must you enable?
  - A. Network Policy Server
  - B. Network Routing Server
  - C. Routing and Remote Access Services
  - D. None of the above. Windows cannot be used as a router.
3. Network Access Protection (NAP) will only work with certain operating systems at the time of Windows 2008 Server release. What operating systems will NAP support?
  - A. Window XP
  - B. Windows XP Service Pack 3
  - C. Windows Vista
  - D. Windows Server 2008
4. Network Access Protection (NAP) can provide network protection to various types of network communications. Which of the following *will not* support NAP?
  - A. RRAS Connections
  - B. DHCP Supported Network
  - C. WINS Supported Network
  - D. IEEE 802.11B Wireless Network

5. The NAP Health Policy Server is responsible for storing health requirement policies and provides health state validation for the NAP Infrastructure. What Windows Server 2008 roles have to be installed for the NAP Health Policy Server to be configured?
  - A. Active Directory Domain Role
  - B. NPS Server Role
  - C. NAP Server Role
  - D. DHCP Server Role
6. NAP Health Policies are a combination of settings for health determination and enforcement of infrastructure compliance. What are the sets of settings that make up the NAP Health Policies?
  - A. Connection Request Policies
  - B. Network Policies
  - C. Health Policies
  - D. Network Access Protection Settings
7. Encrypted Files and Folders are displayed with what color by default in Windows explorer?
  - A. blue
  - B. green
  - C. grayed out
  - D. red
8. Where do you go to configure a secure connection between two nodes in the Windows Firewall with Advanced Security?
  - A. Connection Security Rules
  - B. Inbound Connections
  - C. Outbound Connections
  - D. Monitoring

9. What are the two types of Security Associations that can be monitored in the Windows Firewall with Advanced Security?
  - A. Domain, Quick
  - B. Main, Quick
  - C. Public, Private
  - D. Public, Domain
10. What are the three firewall profiles you can use in the Windows Firewall with Advanced Security?
  - A. Public, Private, Network
  - B. Public, Home, Domain
  - C. Public, Private, Domain
  - D. Public, Work, Domain

## Self Test Quick Answer Key

- |                       |                          |
|-----------------------|--------------------------|
| 1. <b>B, C, and D</b> | 6. <b>A, B, C, and D</b> |
| 2. <b>C</b>           | 7. <b>B</b>              |
| 3. <b>B, C, and D</b> | 8. <b>A</b>              |
| 4. <b>C</b>           | 9. <b>B</b>              |
| 5. <b>B</b>           | 10. <b>C</b>             |

# Chapter 5

## MCITP Exam 646

### 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.

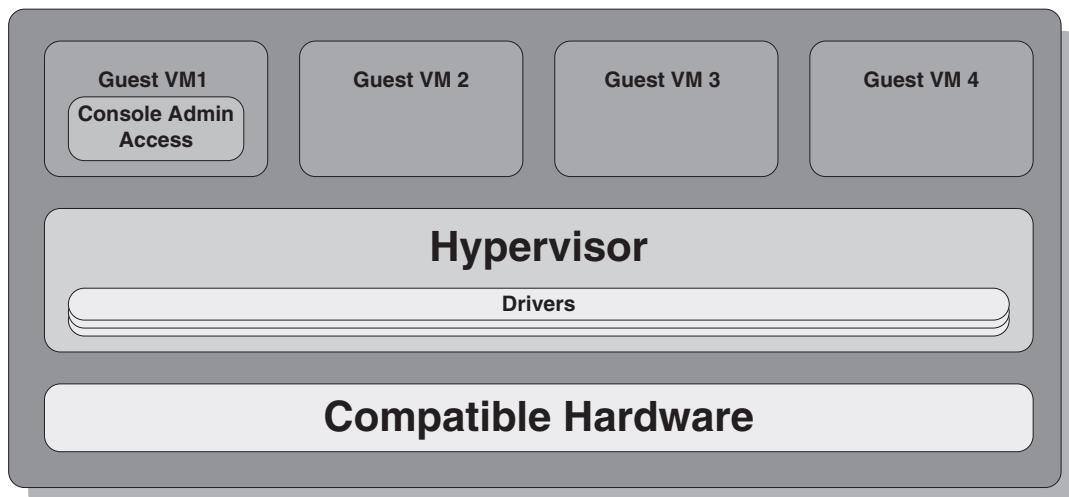
## Microkernelized vs. Monolithic Hypervisor

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 5.1). This configuration has its advantages as well as some key disadvantages.

**Figure 5.1 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

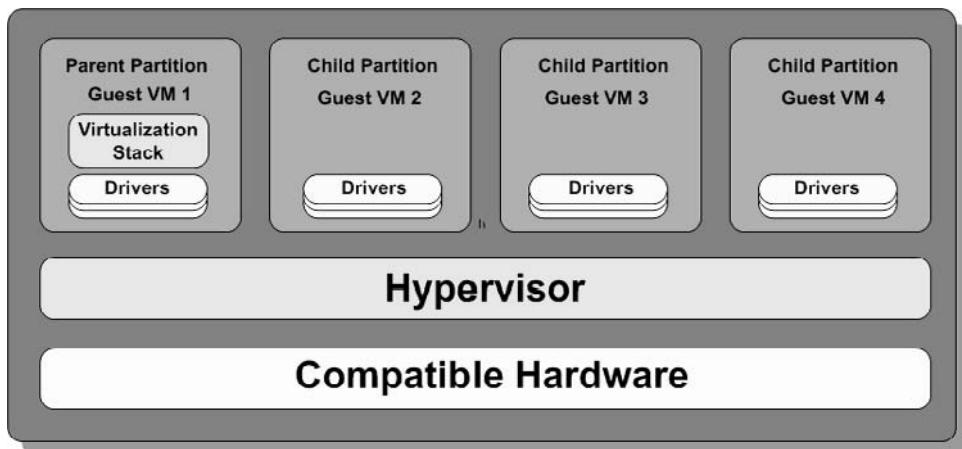
The microkernel-style of hypervisor architecture removes device drivers from the hypervisor layer entirely (see Figure 5.2). The drivers have been relocated to the individual guest operating system partitions, where they run separately for each individual virtual machine. This is the type of hypervisor 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 5.2** 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.

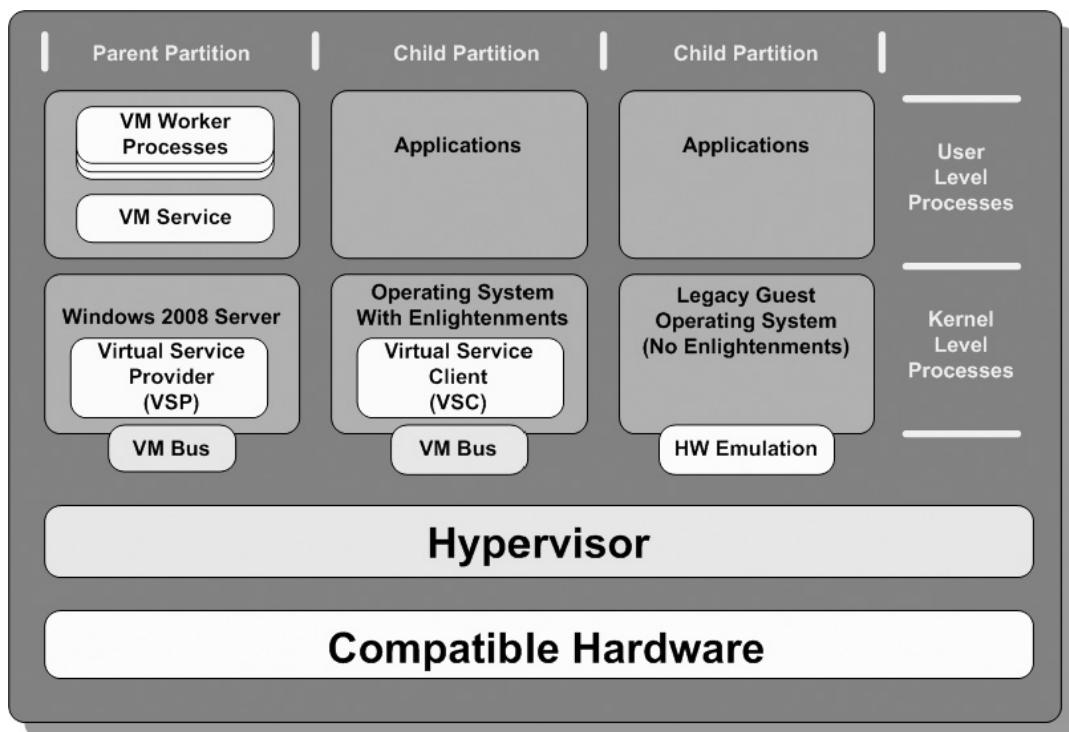
Specifically, the processors required to support these functions are the AMD-V or Intel VT processors. There are detailed vendor-specific listings available showing exactly which processors from each manufacturer will support this functionality; therefore, it is imperative that these references be consulted 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 5.3).

**Figure 5.3** 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 5.4). 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 5.4** 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" tree with "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: "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 showing "Off" as the status and "n/a" for both running time and CPU usage.

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 5.1.

**Table 5.1 Feature Comparison between Windows Server Hyper-V Virtual Server 2005 R2**

<b>Feature Comparison</b>	
<b>Windows Server Hyper-V</b>	<b>Windows Virtual Server 2005 R2 SP1</b>
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
<b>SCVMM 2007 not supported</b> A promised upgrade in the next pending release of SCVMM 2007, due out in mid-2008.	<b>Integration with SCVMM 2007</b> 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.

---

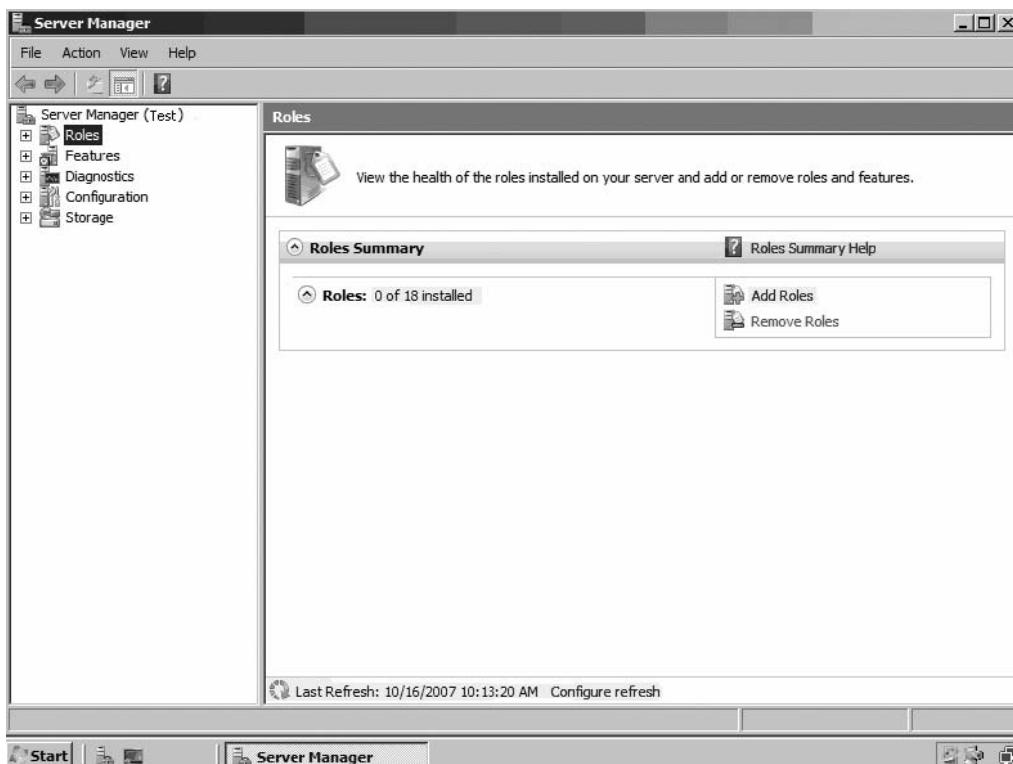
## EXERCISE 5.1

### 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.

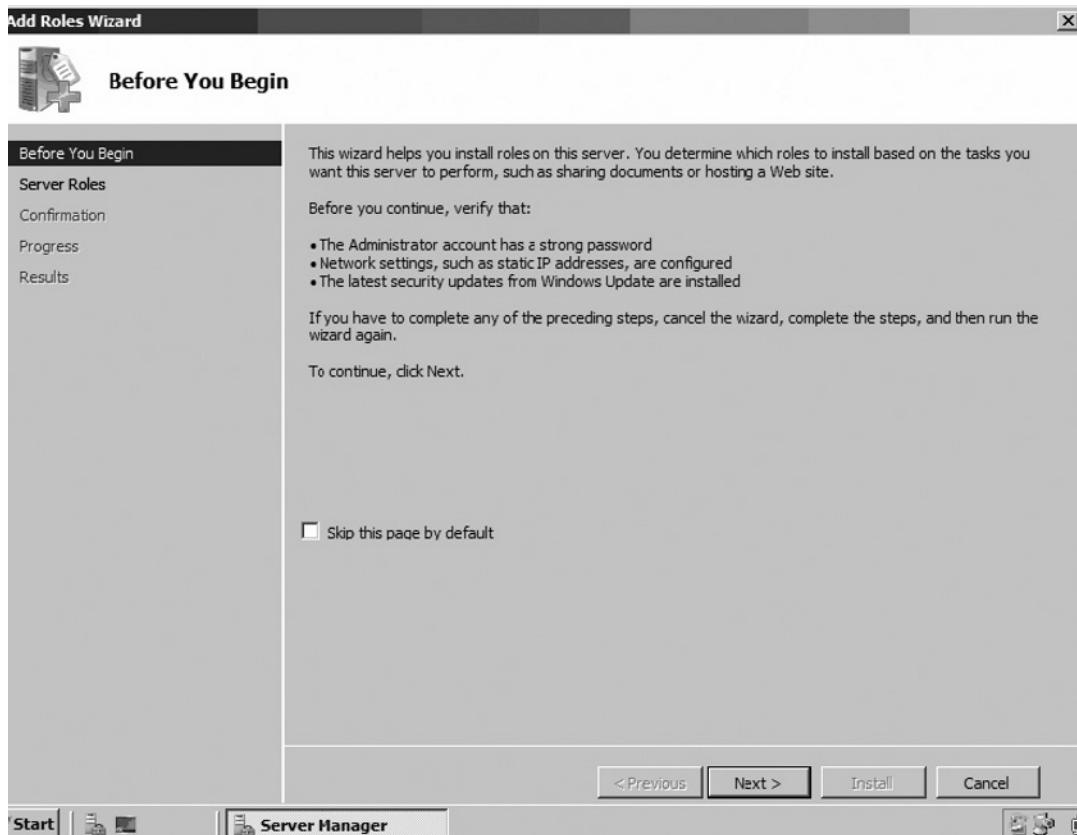
1. Log on to the Windows Server 2008 instance using an account possessing administrative privileges.
2. Install the **Update for Windows Server 2008 KB949219** (either 32 or 64 bit).
3. Reboot the server when prompted.
4. Select **Start | Administrative Tools | Server Manager | Roles**.
5. Select the **Add Roles** link (see Figure 5.5).

**Figure 5.5** Server Manager “Add Roles” Page

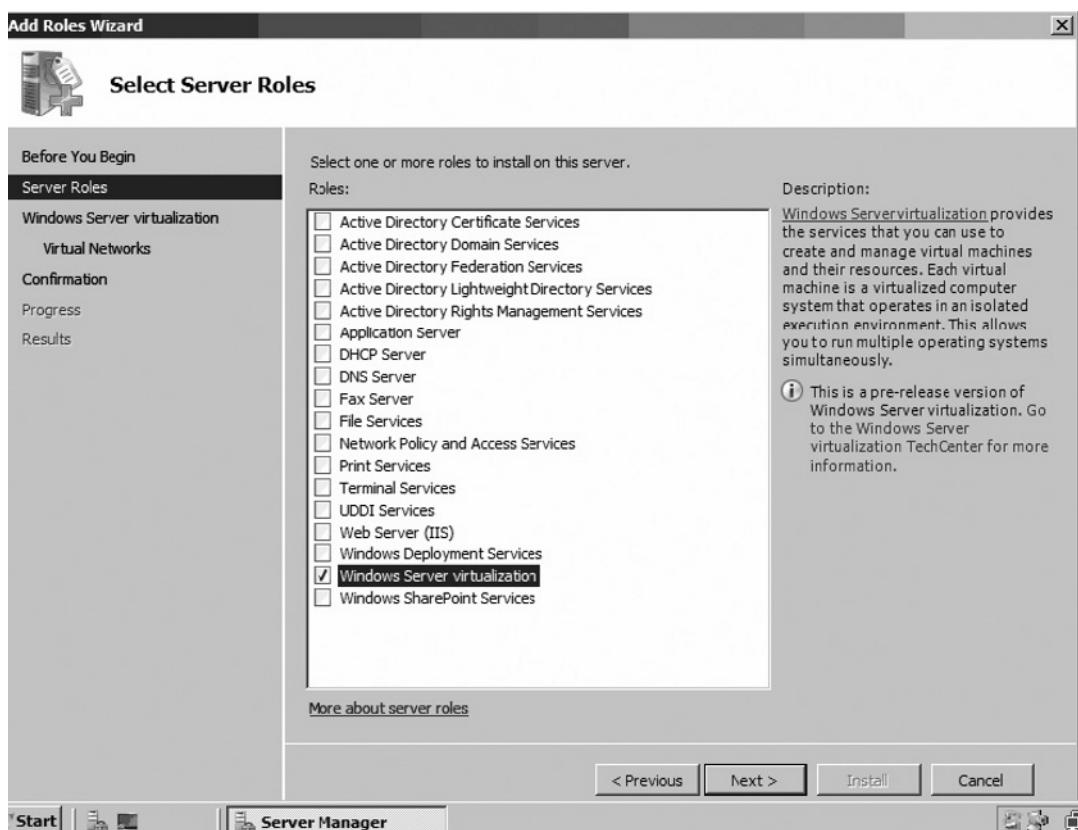


6. On the **Before You Begin** page, ensure prerequisites are met; then click **Next** (see Figure 5.6).

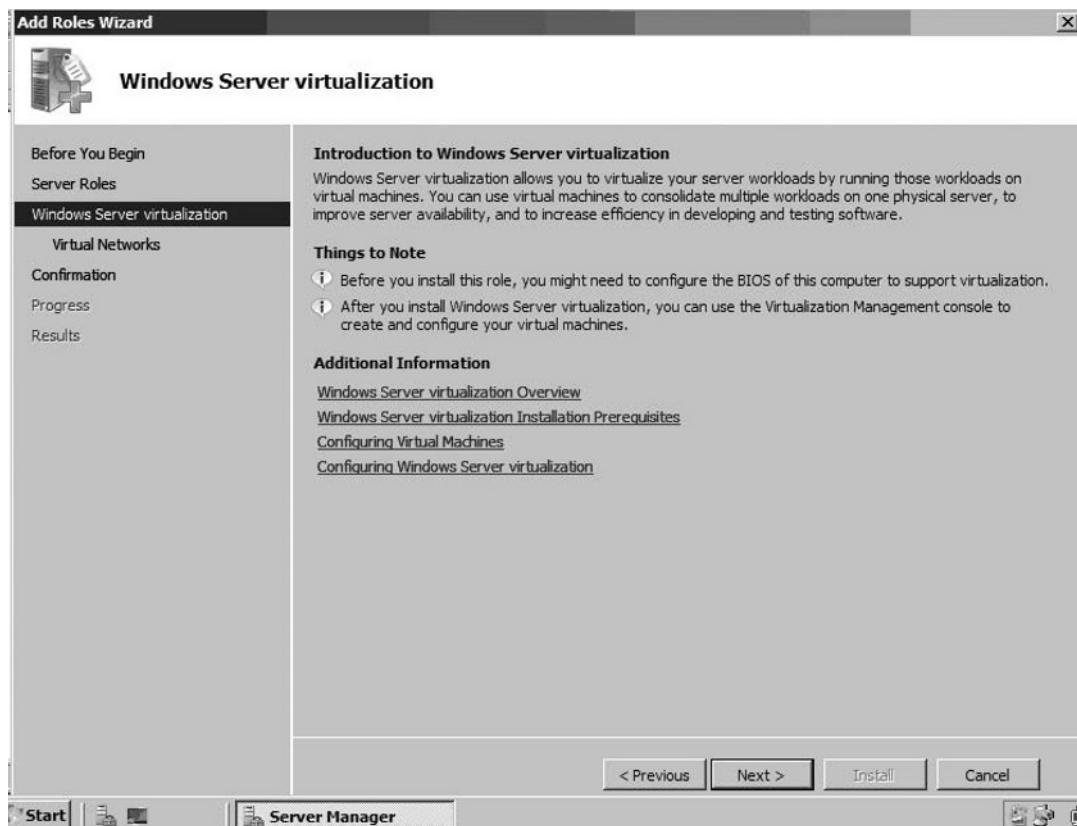
**Figure 5.6** Add Roles Wizard Before You Begin Page



7. On the **Select Server Roles** page, select the role called **Windows Server Virtualization**, then click **Next** (see Figure 5.7).

**Figure 5.7** 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 5.8).

**Figure 5.8** 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 5.9).
10. Once complete, click **Next** to continue.

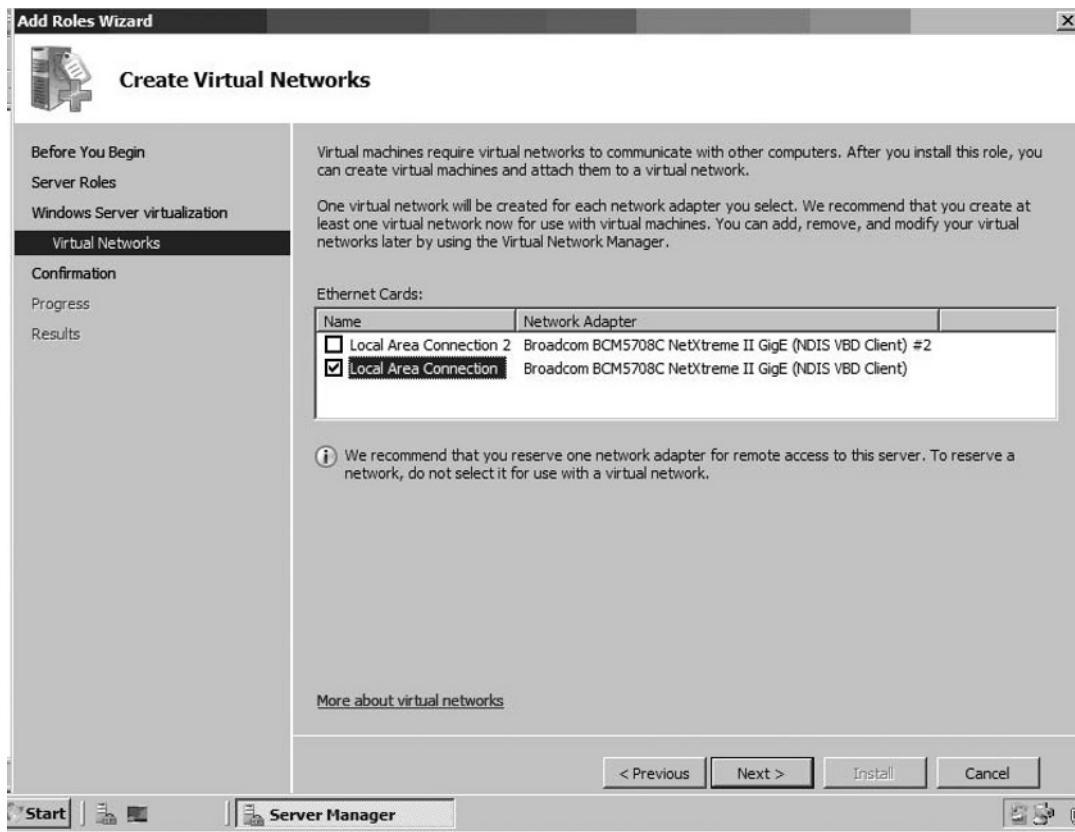
### NOTE

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.

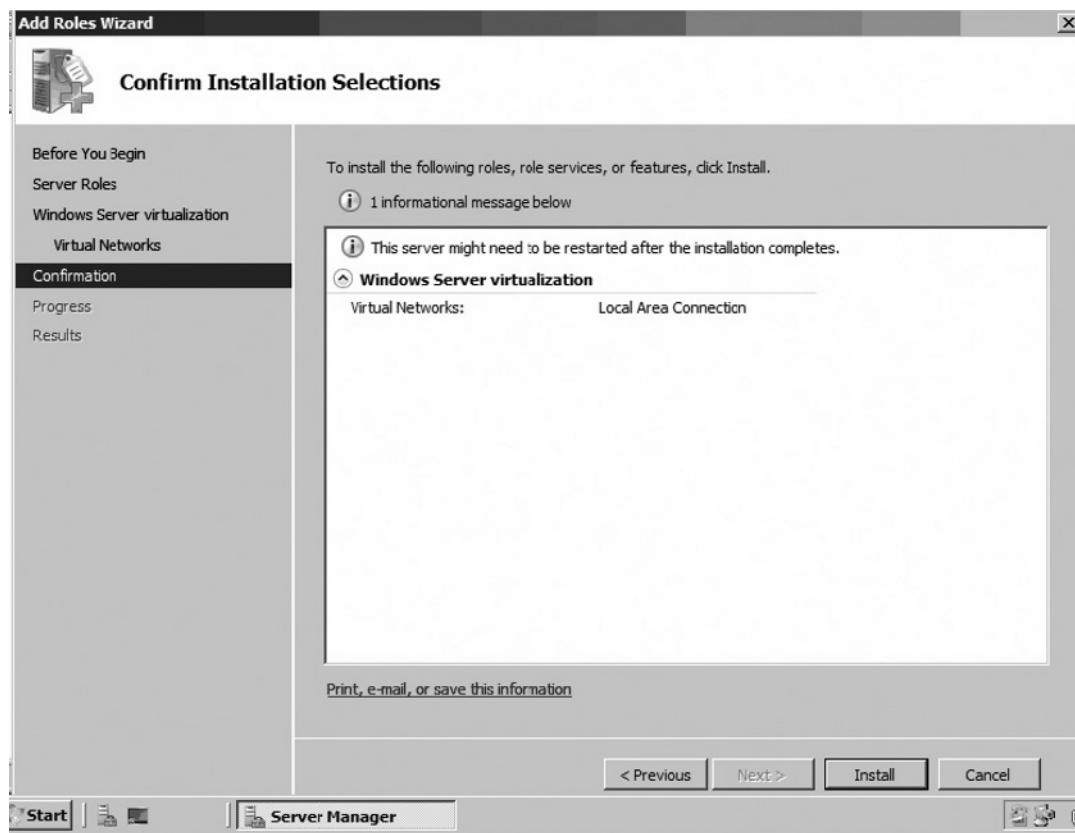
**TEST DAY TIP**

To reserve an adapter for console communication just don't select it this page.

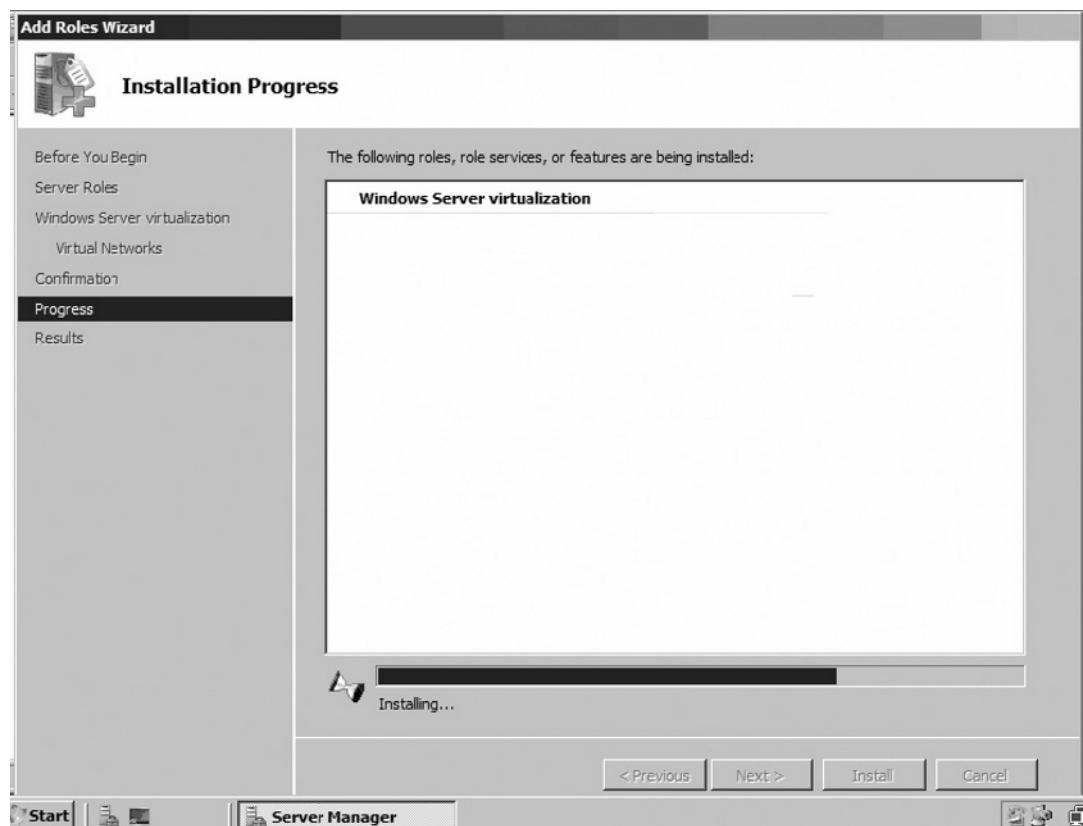
**Figure 5.9 Add Roles Wizard Create Virtual Networks Page**



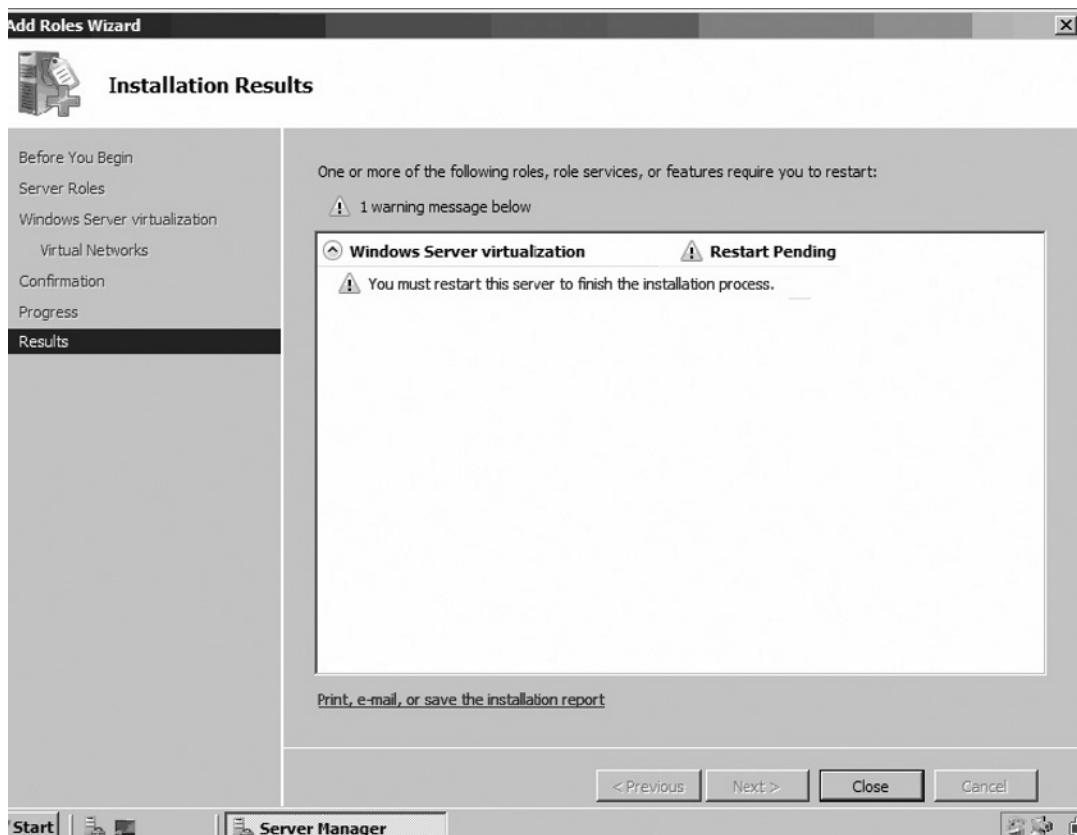
11. The **Confirm Installation Selections** screen, shown in Figure 5.10, displays the results of previous choices. The information most important to confirm is the choice of network adapter. When satisfied with the choices displayed click **Next** to continue.

**Figure 5.10** Add Roles Wizard Confirm Installation Selections Page

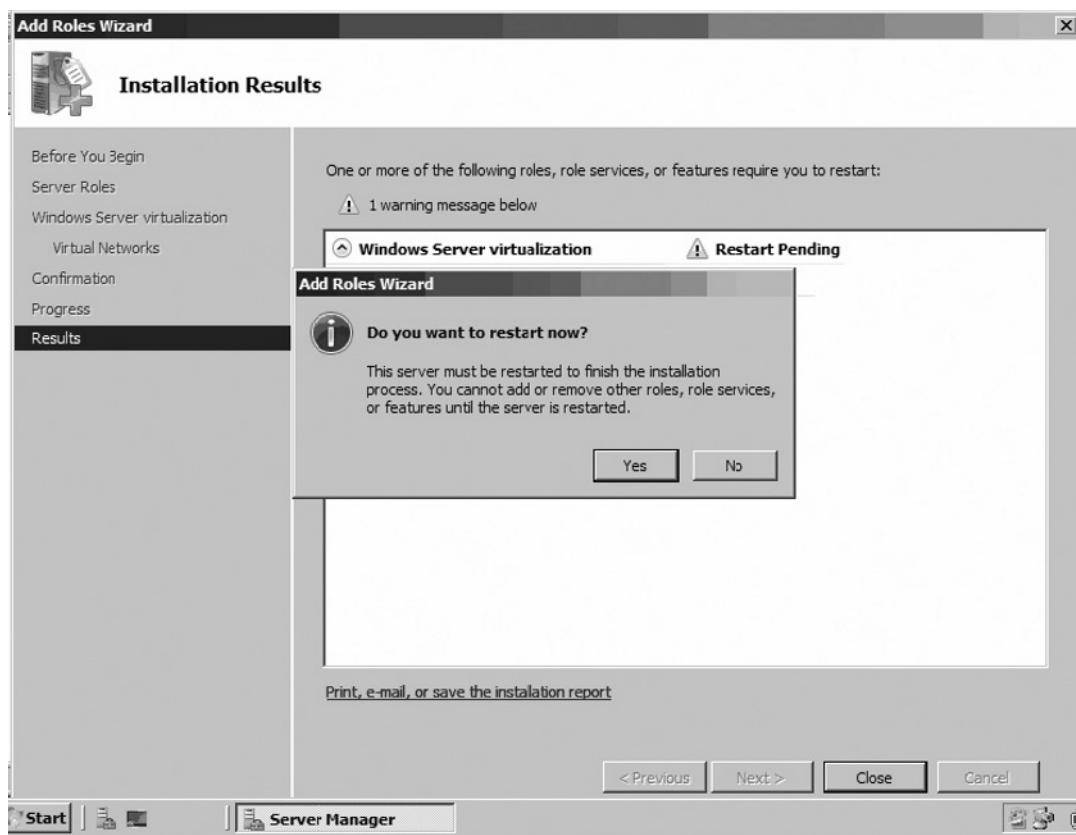
13. The **Installation Progress** screen will then appear showing that the actual installation phase has started (see Figure 5.11).

**Figure 5.11** Add Roles Wizard Installation Progress Page

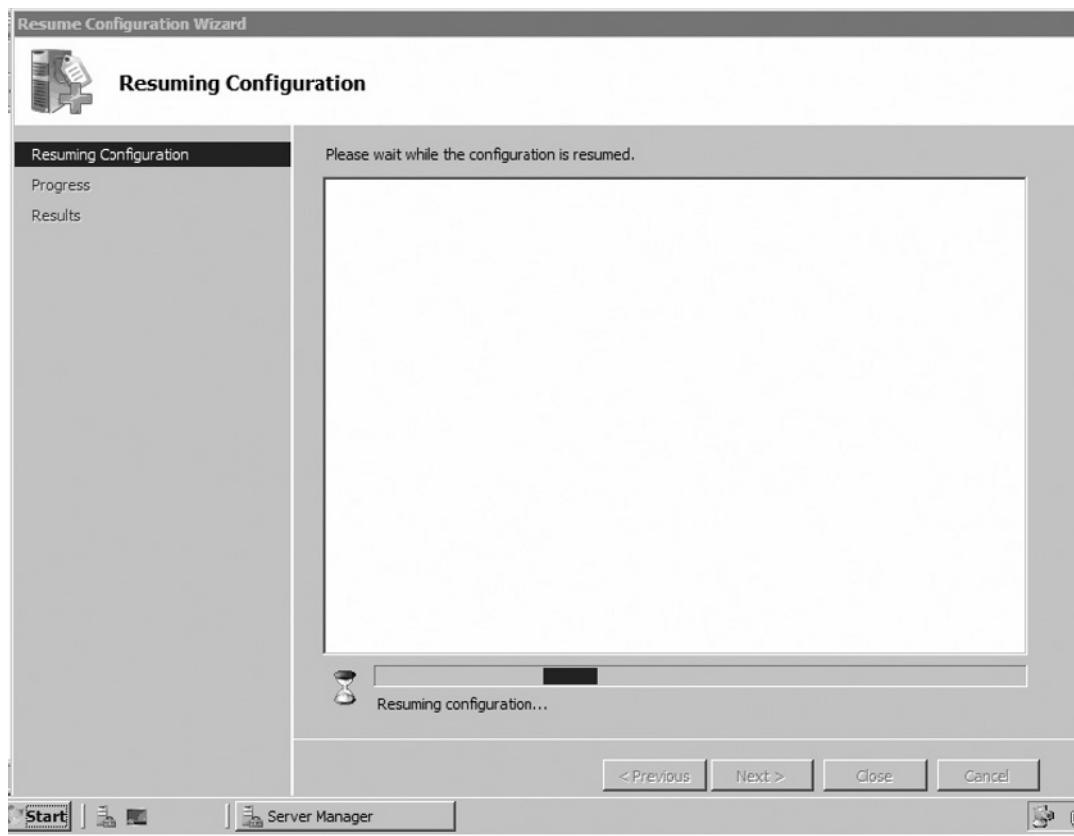
14. Once the **Installation Result** page appears, you will see the notice that a restart is pending. Select **Close** at the bottom to continue with the installation (see Figure 5.12).

**Figure 5.12** Add Roles Wizard Installation Results Page

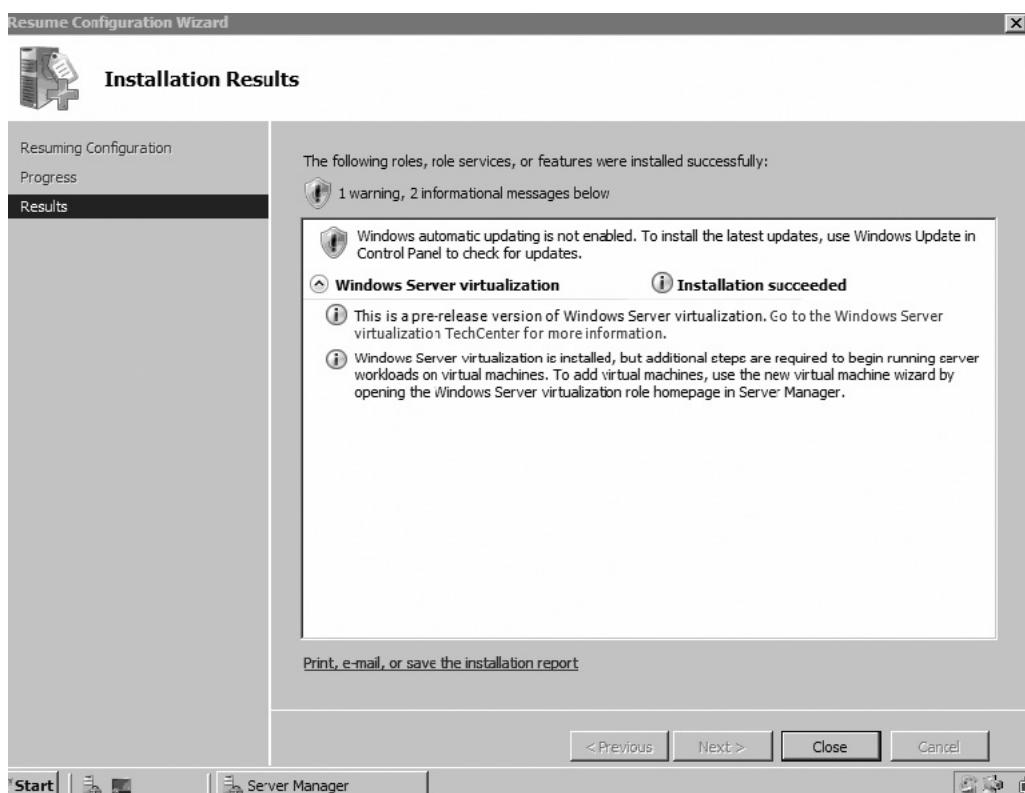
15. Once the **Installation Results** page appears you will see the notice that a restart is pending. Select **Close** at the bottom to continue with the installation (see Figure 5.13).

**Figure 5.13** Add Roles Wizard Installation Results

16. After the reboot, log on again. The installation will resume, as shown in Figure 5.14.

**Figure 5.14** 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 5.15).

**Figure 5.15** 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 5.16):

- **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 5.16** 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 5.2

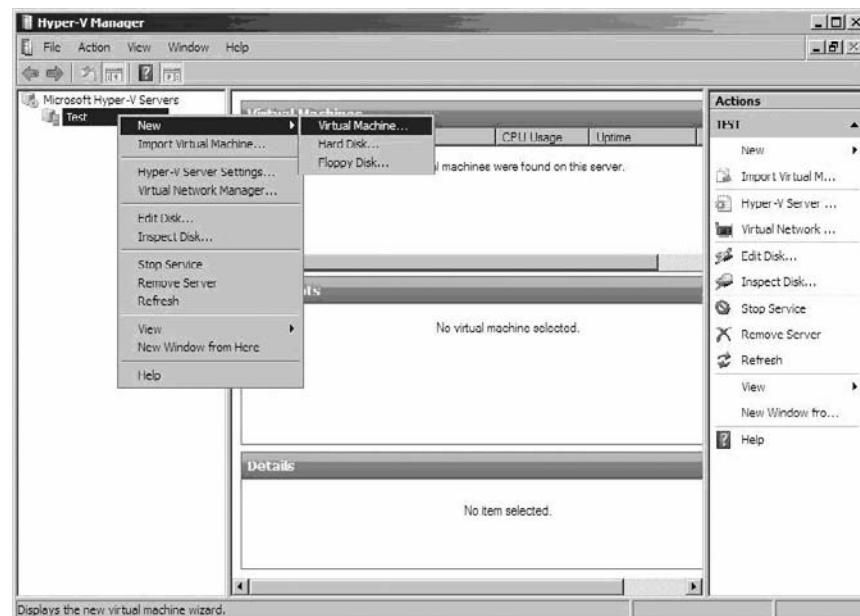
### CREATING A VIRTUAL MACHINE USING WINDOWS SERVER 2008's STAND-ALONE HYPER-V MANAGER CONSOLE

1. Log on to Windows Server 2008 using an account with administrative privileges.
2. Select **Start | Administrative Tools | Windows Server Virtualization.**

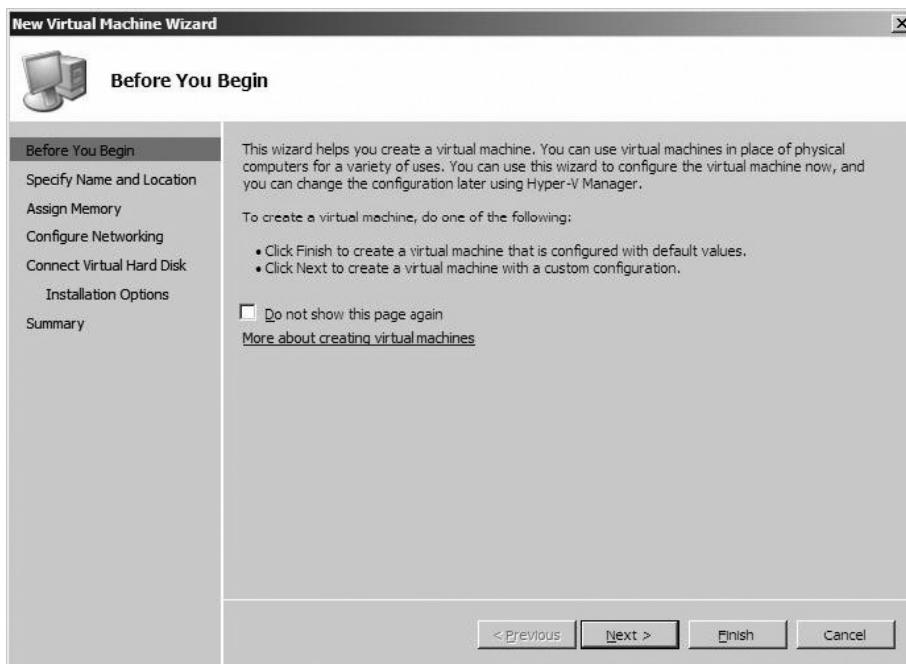
#### NOTE

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 5.17).

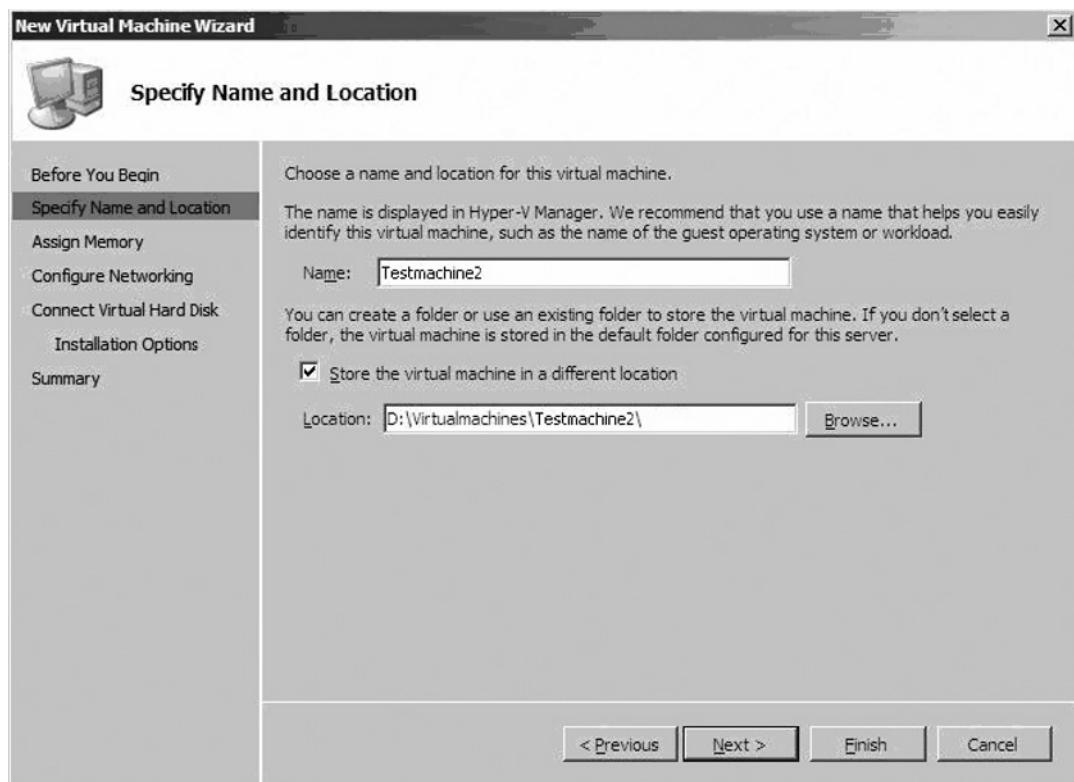
**Figure 5.17** The Hyper-V Manager Console

4. The **Before You Begin** page is informational. Select **Next** to proceed (see Figure 5.18).

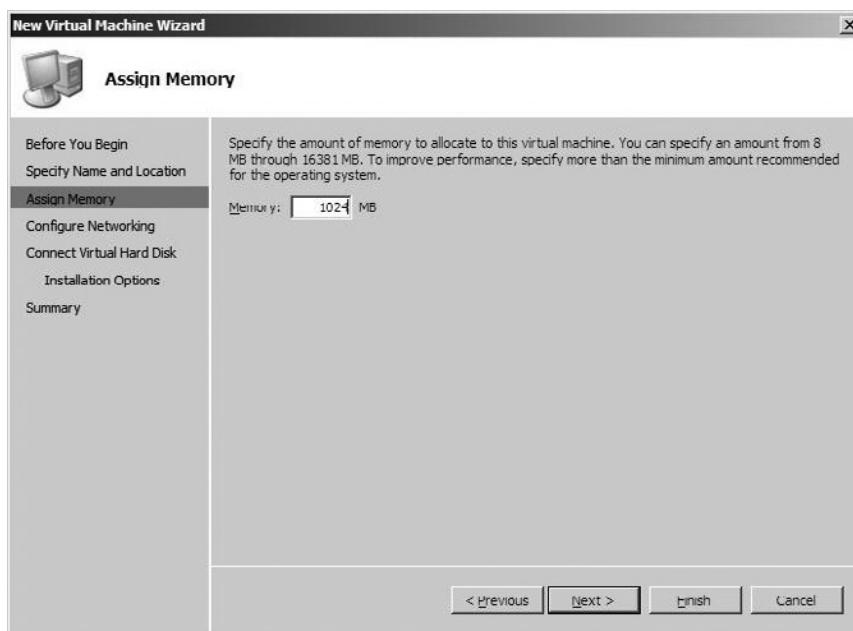
**Figure 5.18** New Virtual Machine Wizard Before You Begin Page

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 5.19).

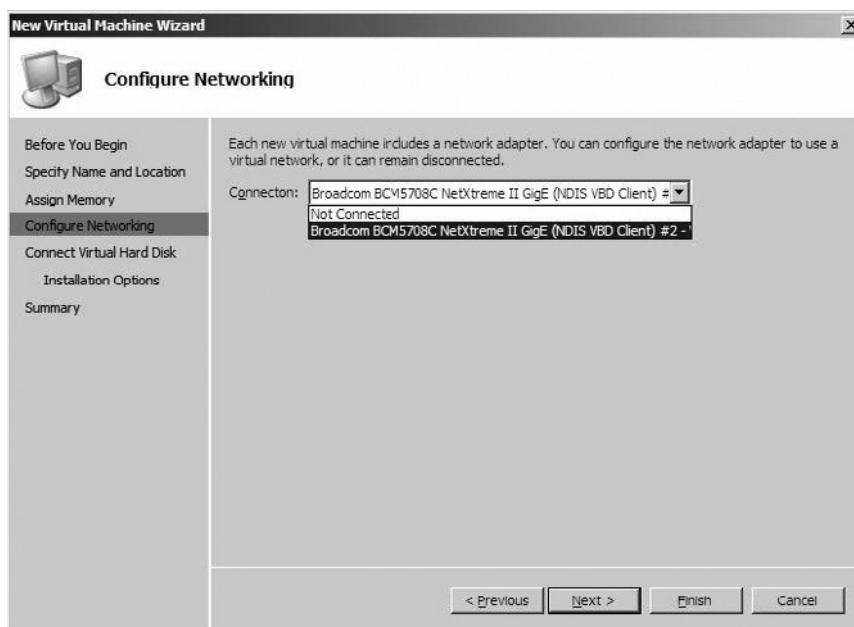
**Figure 5.19** New Virtual Machine Wizard Specify Name and Location Page



6. In the **Assign Memory** page, allocate the VM's memory and then select **Next** (see Figure 5.20).

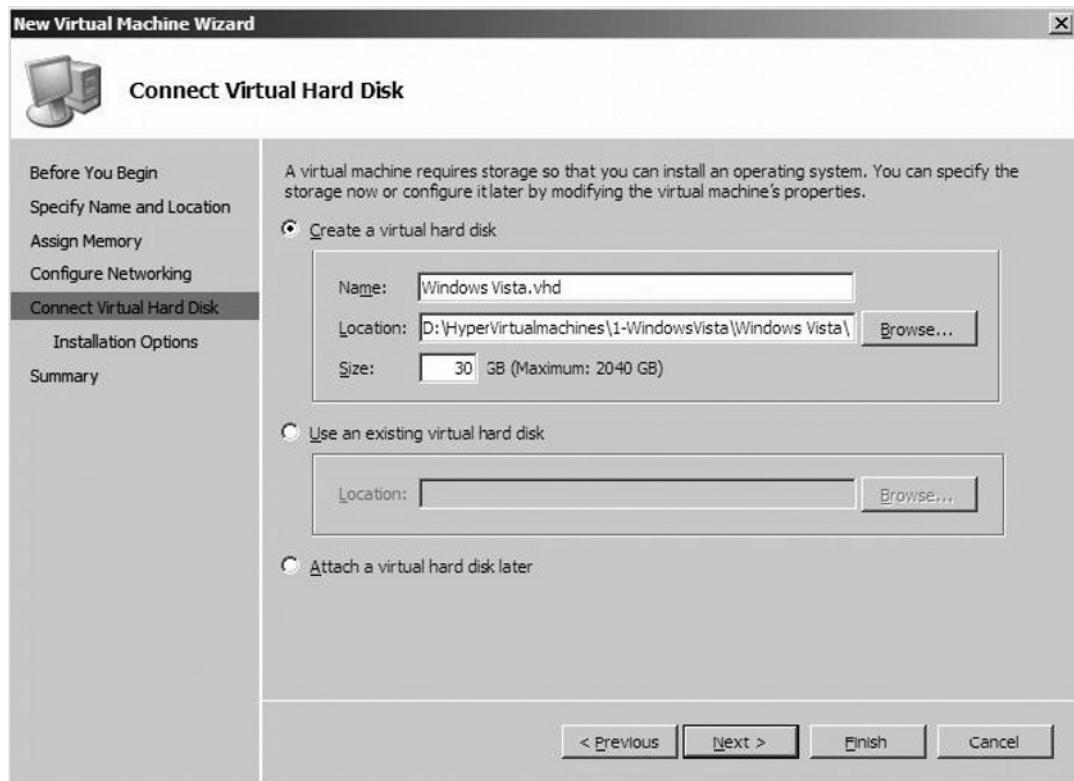
**Figure 5.20** New Virtual Machine Wizard Assign Memory Page

7. In the **Configure Networking** page, choose the network adapter that you want the virtual machine to use for network communication (see Figure 5.21).

**Figure 5.21** New Virtual Machine Wizard Configure Networking Page

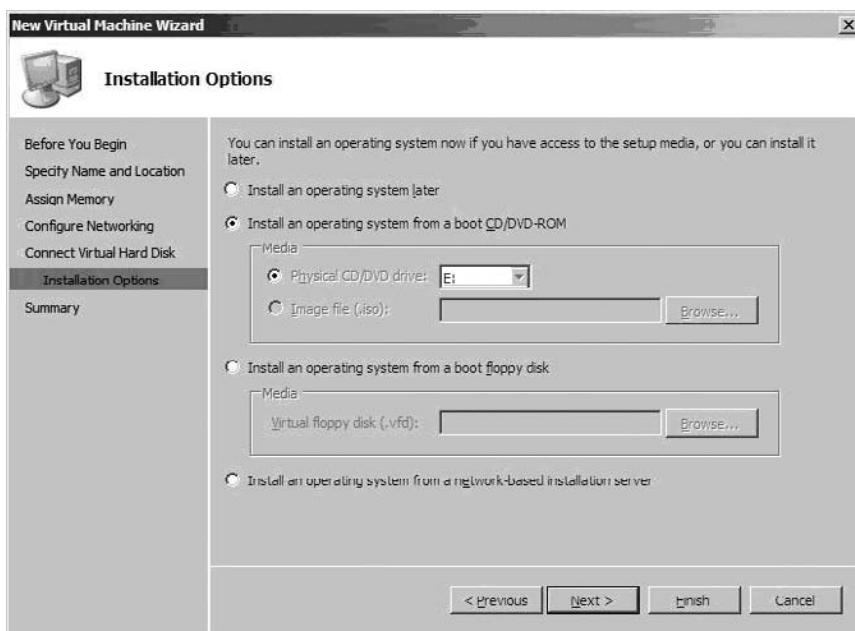
8. In the **Connect Virtual Hard Disk** page, provide the file name, storage location, and size of the .vhd virtual disk file to be attached to the new VM then select **Next** (see Figure 5.22).

**Figure 5.22** 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 5.23).

**Figure 5.23** New Virtual Machine Wizard Installation Options Page



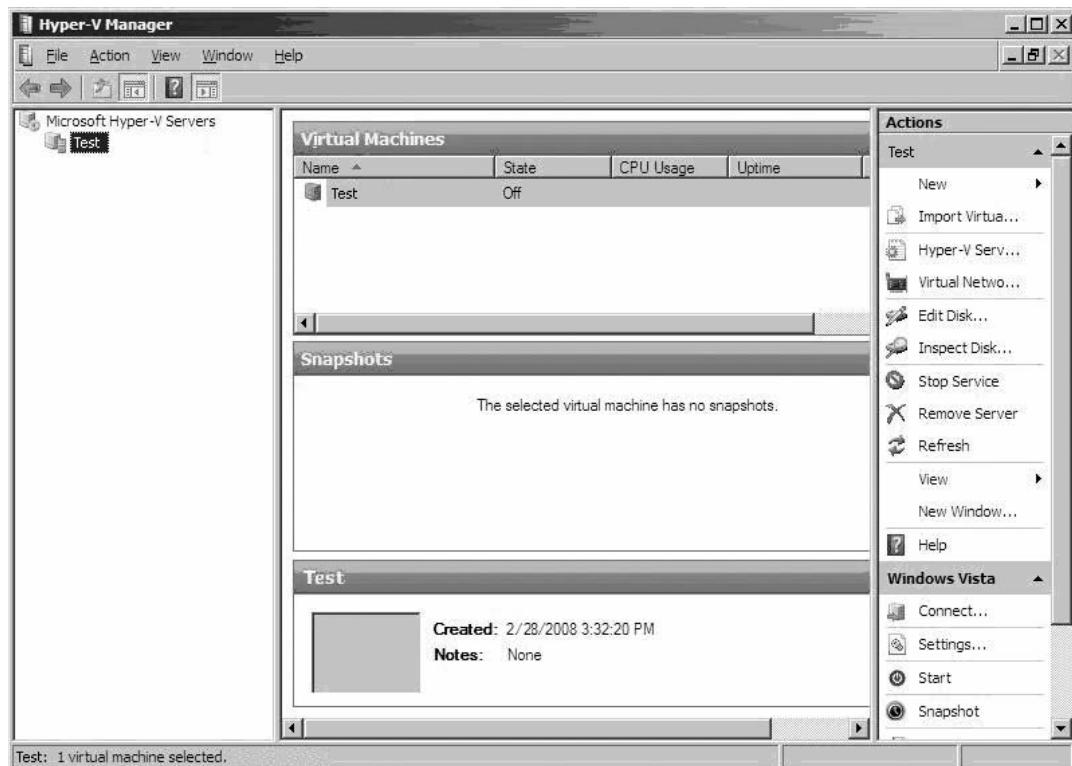
10. After reviewing all selections select **Finish** to create the virtual machine (see Figure 5.24).

**Figure 5.24** New Virtual Machine Wizard Completing the Wizard Page

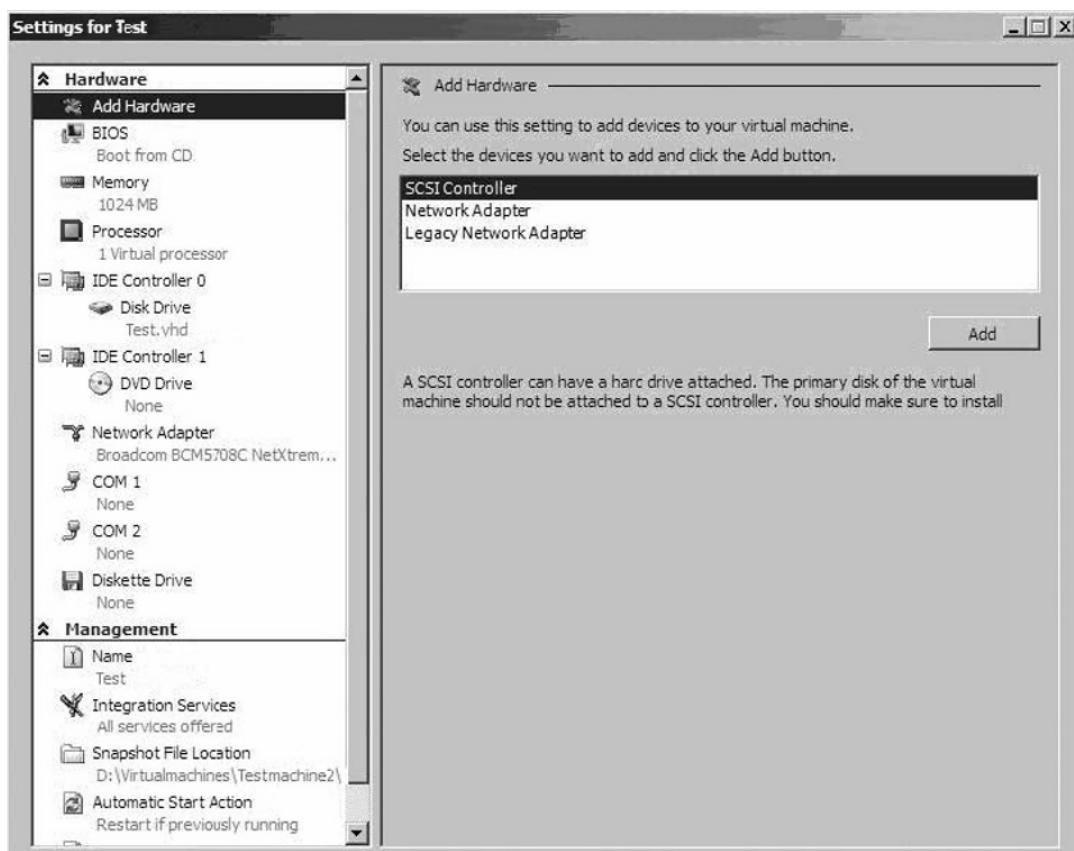


11. Once completed, reopen **Hyper-V Manager** to view the newly created virtual machine (see Figure 5.25).

**Figure 5.25** The Hyper-V Manager Console



12. Right click on the new virtual machine and select **Settings** to view available options (see Figure 5.26).

**Figure 5.26** 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 5.27).
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 5.27** 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 5.2). 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 5.2 Feature Comparison between Windows Server Virtualization and ESX Server**

<b>Feature Comparison</b>		
<b>Feature</b>	<b>VMware ESX 3.X</b>	<b>Windows Server Hyper-V</b>
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 5.2 Continued.** Feature Comparison between Windows Server Virtualization and ESX Server

<b>Feature Comparison</b>		
<b>Feature</b>	<b>VMware ESX 3.X</b>	<b>Windows Server Hyper-V</b>
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.

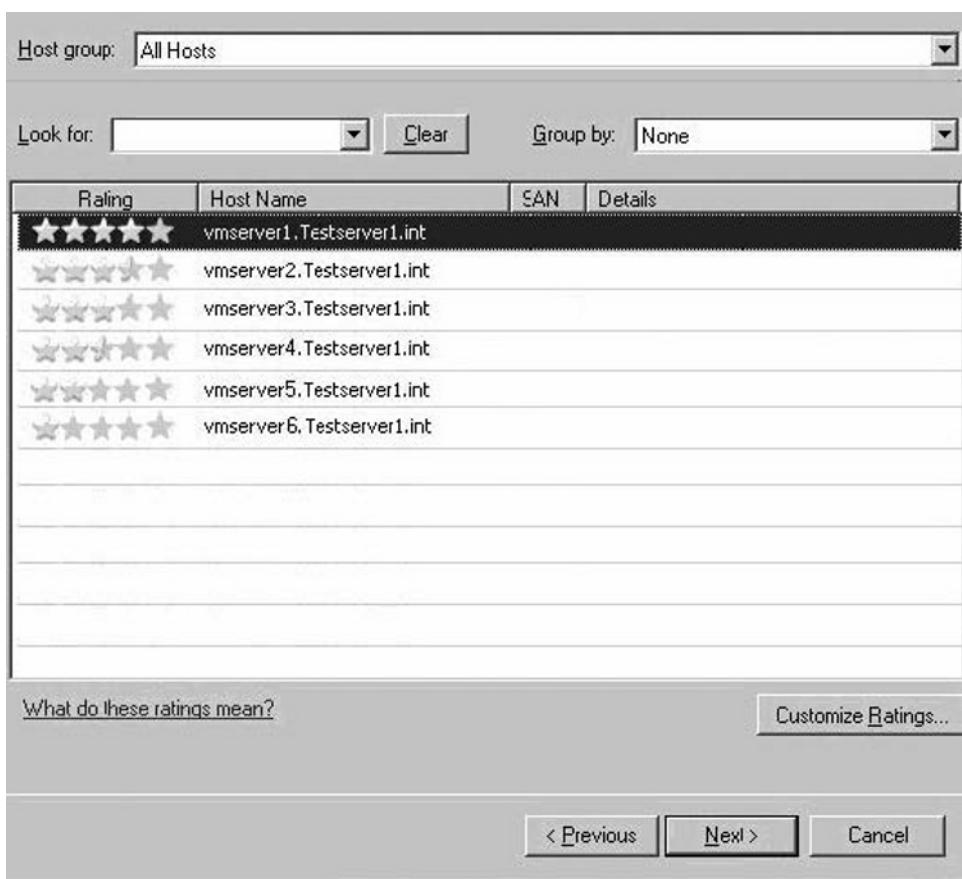
The virtual resource management tool discussed shortly provides a wizard-based capability that allows for a virtual machine's ideal placement to be considered and assessed based not only upon the anticipated resource utilization, but also on the intended goal of the administrator in choosing the placement. 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 5.28):

- 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 5.28** 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 .vhf 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

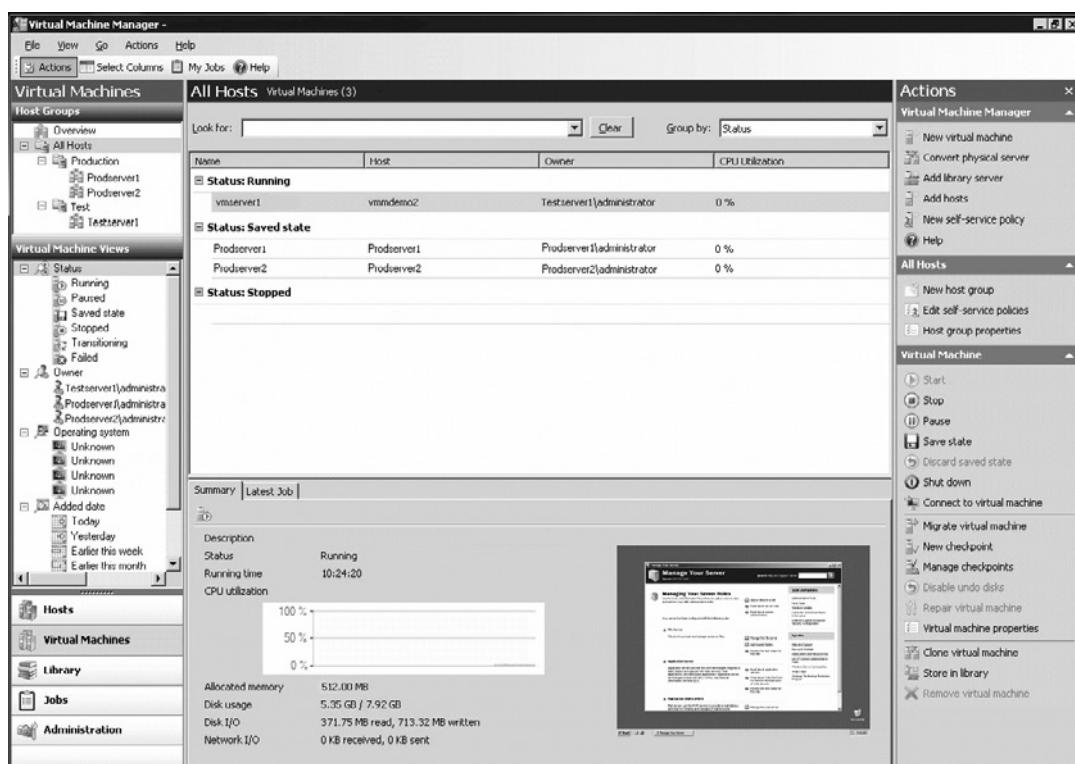
The System Center Virtual Machine Manager Administrator Console provides access to all the tools needed to perform virtual machine management for the following virtualized assets:

- 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 5.29).

**Figure 5.29** 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.

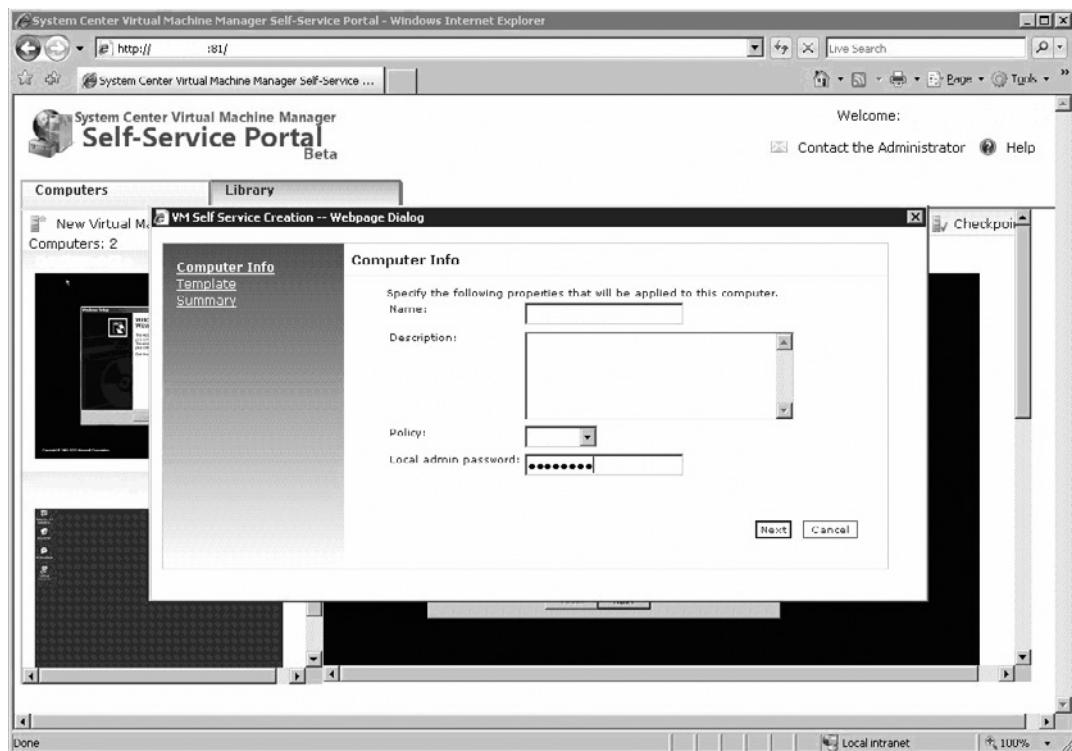
## Windows PowerShell Command-Line Interface

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 5.30). 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 5.30** 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 5.2, 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.

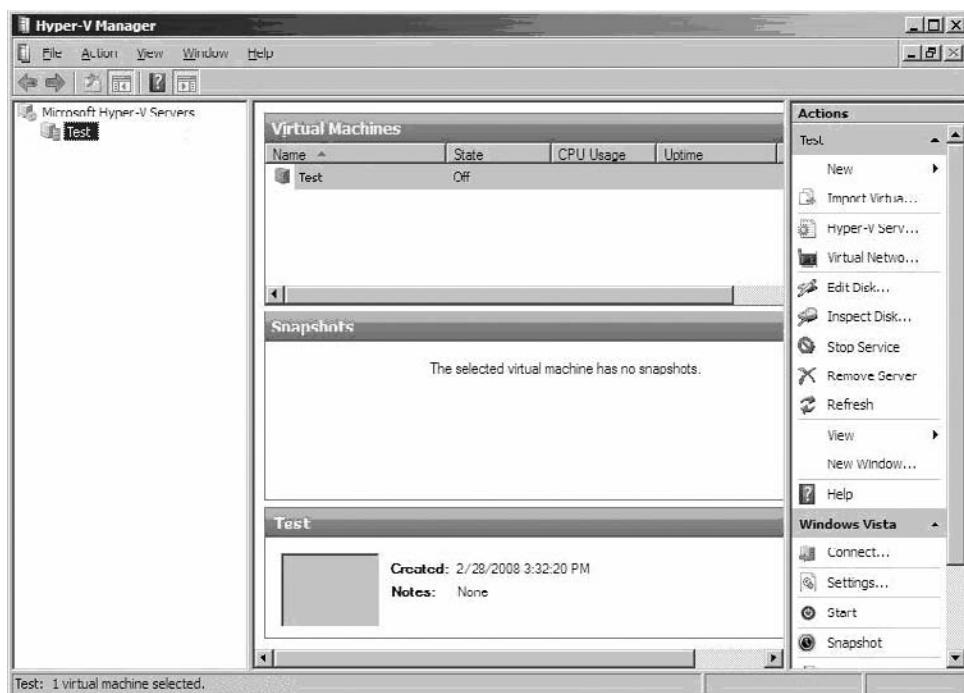
## Stand-Alone Virtualization Management Console

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 5.31).

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 5.31** 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 .vhd format. It does possess the additional ability to convert VMware-based .vmdk format files into the .vhd 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>B</b>    | 6. <b>D</b>       |
| 2. <b>B, D</b> | 7. <b>B</b>       |
| 3. <b>C</b>    | 8. <b>A, B, C</b> |
| 4. <b>A</b>    | 9. <b>D</b>       |
| 5. <b>C</b>    | 10. <b>C</b>      |

This page intentionally left blank

# Chapter 6

## MCITP Exam 646

### Application and Data Provisioning

#### Exam objectives in this chapter:

- Provisioning Applications
- System Center Configuration Manager
- Provisioning Data

#### Exam objectives review:

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

# Introduction

Microsoft has come a long way with terminal services since the Microsoft Windows NT 4.0 Server Terminal Service Addition. In Microsoft Windows 2008 Server, Microsoft has stepped forward and added a lot of new features to better compete with other terminal service vendors. At one time, Microsoft terminal services did not have the ability to provision applications and publish them without using another third party program such as Citrix.

Another hot topic in information technology today is server and application virtualization. Basically, virtualization allows us to take a server and partition it into many servers. Some of the new virtualization technologies from Microsoft include Microsoft Virtual Server 2005 and Microsoft Hyper-V solution. There are many reasons why you would want to consider implementing this into your current IT infrastructure. We will look at these reasons later in this chapter along with the comparisons of Microsoft Virtual Server 2005 and Microsoft Hyper-V.

Finally, in this chapter we are going to look at the new Microsoft System Center Configuration Manager 2007. Formerly known as Microsoft Systems Management Server, Microsoft System Center Configuration Manager 2007 enables you to assess, deploy, and update your clients, servers, and mobile devices across IT systems in physical, virtual, distributed, and mobile environments. Microsoft System Center Configuration Manager 2007 is a separate product from Microsoft Windows 2008 Server and must be purchased and licensed separately.

## EXAM WARNING

It is highly recommended that while studying this book, you should also do all of the exercises via hands-on labs. You can download a copy of Windows 2008 Server Enterprise Edition, Microsoft Virtual PC 2007, and Microsoft System Center Configuration Manager 2007 for free from the Microsoft Web site. Microsoft Virtual PC 2007 is free and all of the needed software has 180 day evaluations available for download. Go out and download these three items and design your own virtual network on your desktop PC. During the exam you will be asked to do hands-on scenario-based questions. The best way to prepare for these types of questions is to do as much hands-on training as possible.

# Provisioning Applications

In this first section, we are going to look at the new Microsoft Windows 2008 Server terminal services features. These new features not only allow us to just provide application executables (like in Microsoft Windows 2003 Server), but also lets us provision the applications for performance and reliability. You will notice right away that terminal services have been redesigned. Some of the new and old features that have been changed include the following:

- Microsoft Terminal Service Gateway
- Microsoft Terminal Service Session Broker
- Microsoft Terminal Services RemoteApp
- Microsoft Terminal Services Web Access

## TEST DAY TIP

Information in this chapter will include many new terms that will need to be memorized for the exam. I would suggest using a notebook and keeping track of these definitions as you work through this chapter. On test day, this will make a great review tool to glance over before heading into the testing center.

## Terminal Server Infrastructure

Microsoft has added many new features to terminal services as we discussed above. To better present the information you will need to pass this exam, let's break the material down into separate sections to get a better understanding of the new features and changes that have been implemented. We will first look at the components and then bring it all together.

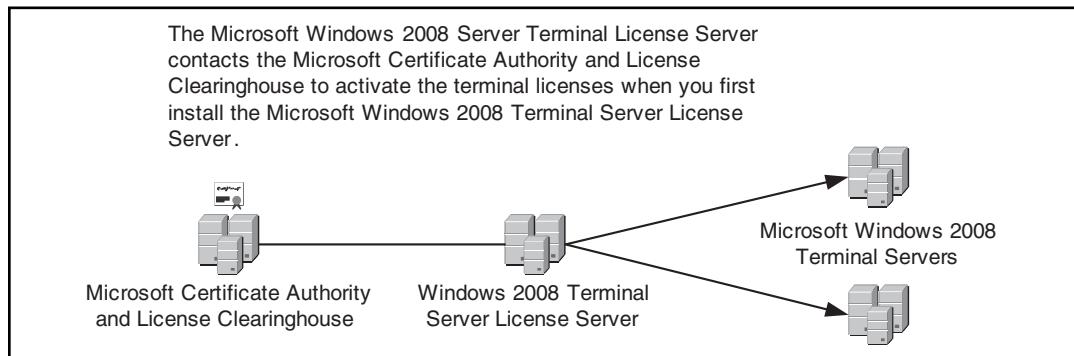
### Terminal Server Licensing

Terminal Services Licensing manages the terminal services client access licenses in your network infrastructure—to operate Terminal Services you need at least one Terminal Server License Server. Many of you that have worked with Microsoft Windows 2003 Server Terminal Services may remember how per device licensing could be hard to manage—having to reset the device client access licenses. In Microsoft Windows Server 2008 Server changes have been made to allow

correcting these problems without having to contact the Microsoft License Clearinghouse to perform a license revocation. In Microsoft Windows 2008 Server, you still need to contact the Microsoft License Clearinghouse to activate your terminal server licenses—see Figure 6.1. Other improvements to the Microsoft Windows 2008 Server Terminal Server Licensing include:

- New Management and Reporting Features
- Troubleshooting Tools
- License Server Discovery Process
- Per-Device Client Access License Revocation
- Per-User Client Access Licensing Tracking in Active Directory

**Figure 6.1** Terminal License Server Activation



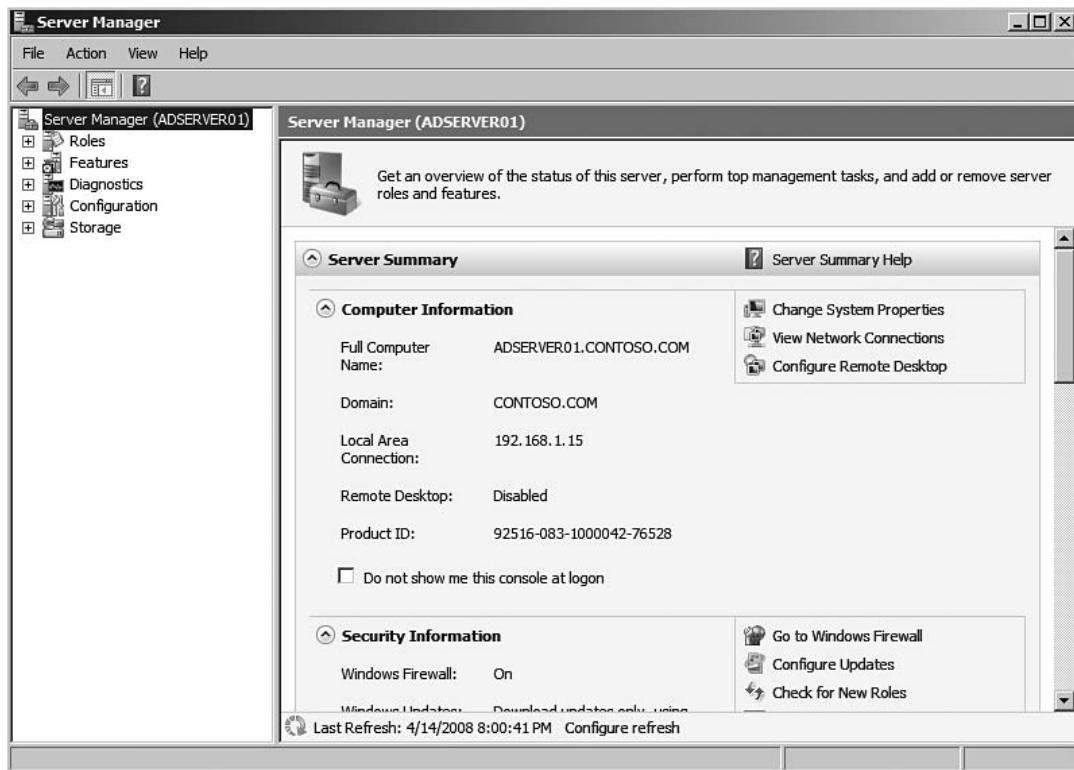
## EXERCISE 6.1

### INSTALLING MICROSOFT WINDOWS 2008 SERVER TERMINAL LICENSE SERVER

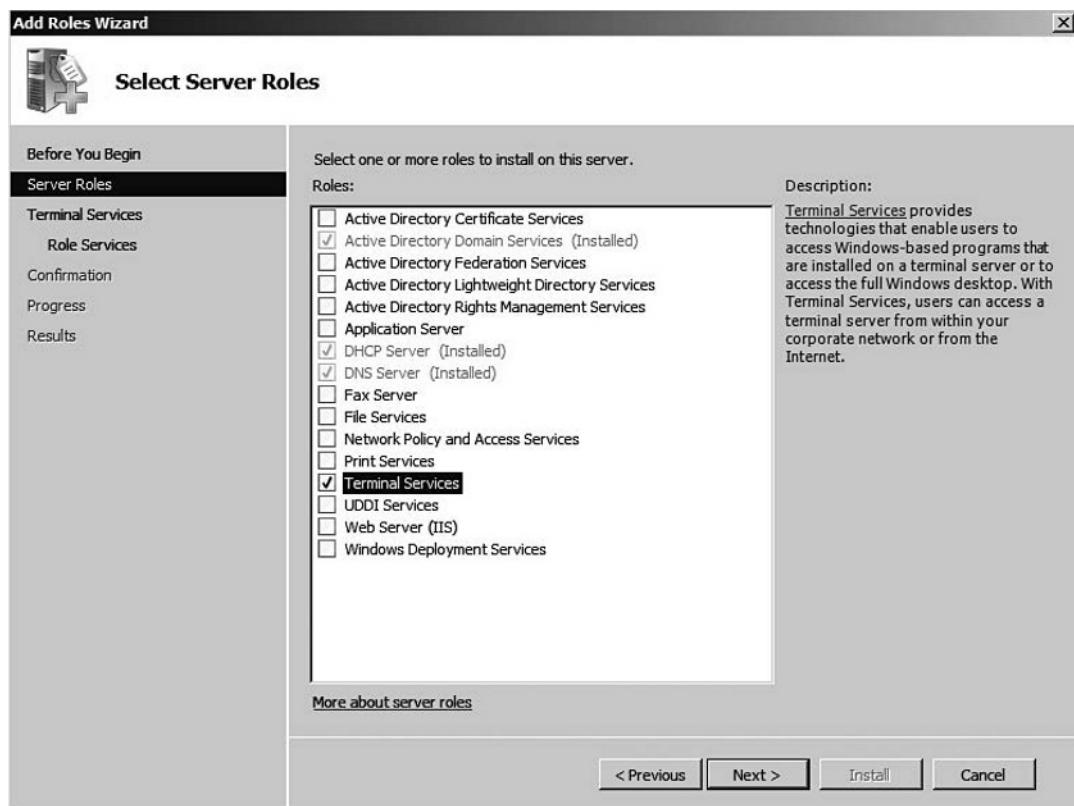
Note: The lab environment is set up with the following servers: ADSERVER01, TSSERVER01, and Windows Vista TSClient. We will use ADSERVER01 as our Microsoft Windows 2008 Server Terminal License Server.

In this lab, we are going to install the Microsoft Windows 2008 Server Terminal License Server on server ADSERVER01. ADSERVER01 is an Active Directory server in the CONTOSO Active Directory domain.

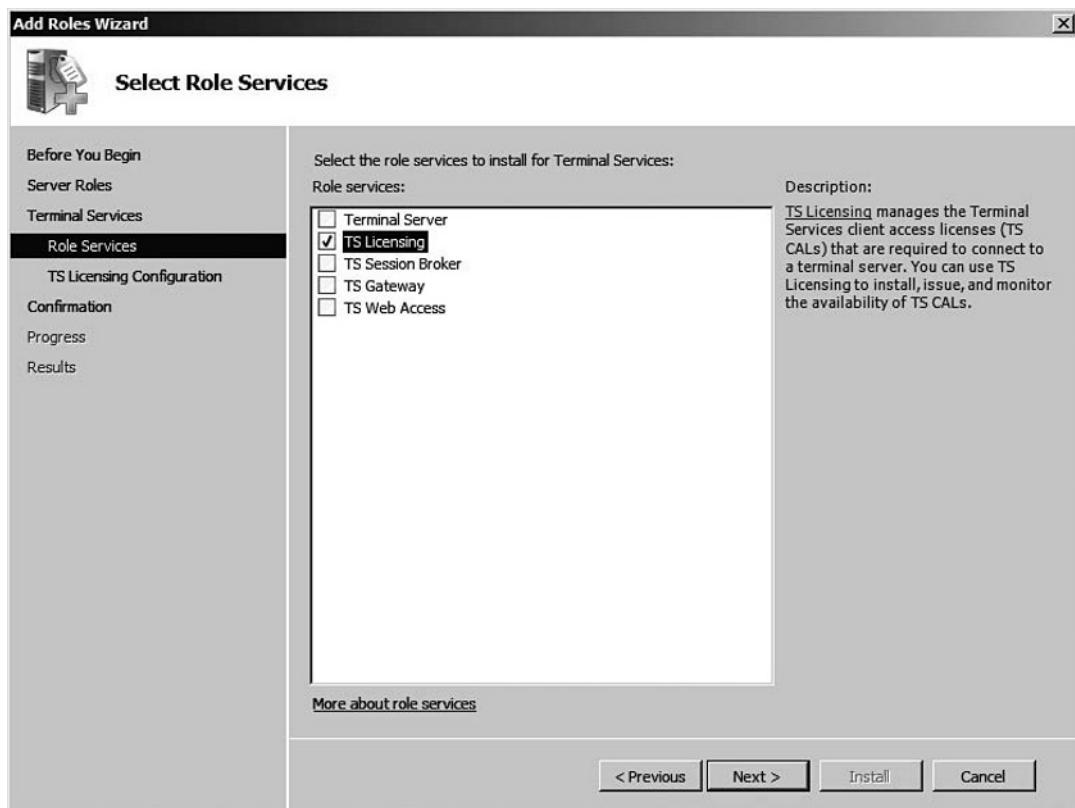
1. First, we will need to open the **Server Manager**. To do this, click on **Start** then **Server Manager** at the top of the Start Menu—see Figure 6.2.

**Figure 6.2 Microsoft Windows 2008 Server Manager**

2. Within the Server Manager click **Roles**, then click **Add Roles**.
3. At the next screen, click **Next** to continue.
4. Select the **Terminal Service** role and click **Next**. See Figure 6.3.

**Figure 6.3** Add Roles Wizard

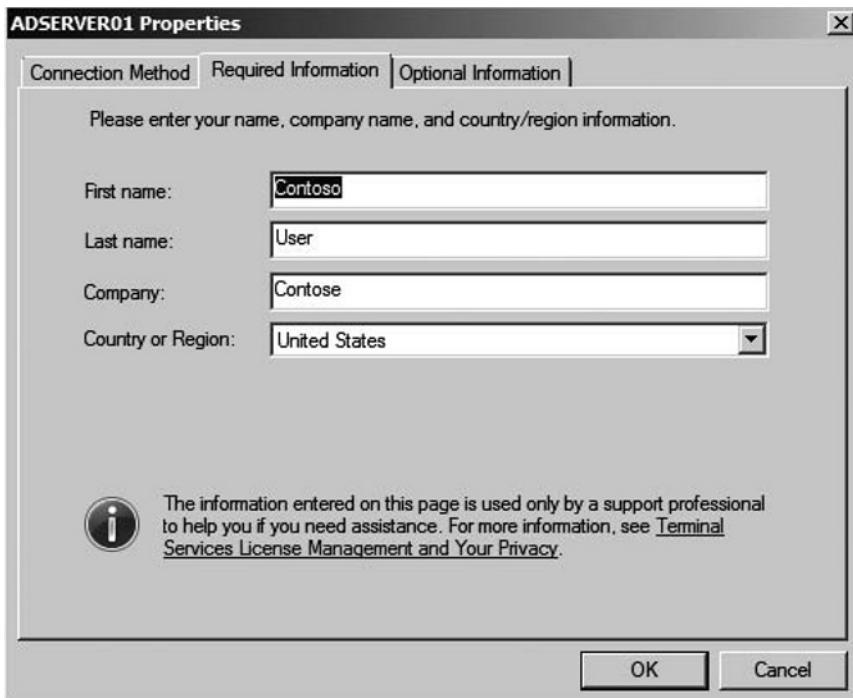
5. The next window is an **Introduction to Terminal Services**—click **Next**.
6. At the **Select Role Services** window, select **TS Licensing**—see Figure 6.4. Click **Next** to continue.

**Figure 6.4 Select Role Services**

7. Make sure **This domain** is selected in the **Configure Discovery Scope for TS Licensing** and click **Next**. Note: Terminal Services License Server Discovery can take place in a Workgroup, Domain, or Forest.
8. Look over the **Confirm Installation Selections** window and then click **Install**.
9. The **Installation Results** window comes up after the installation completes. Make sure TS Licensing Role was successfully installed. Click **Close**.
10. Click **File**, and then **Exit** to close the **Server Manager**.
11. Next, we will need to activate the TS Licensing server. Click **Start | Administrative Tools | Terminal Services | TS Licensing Manager**.
12. Right-click the server in the **TS Licensing Manager** and click **Properties**.

13. Select the **Required Information** tab and fill in the information—see Figure 6.5. Click **OK** when finished.

**Figure 6.5** Server Properties



14. Right-click the server in the **TS Licensing Manager** and click **Activate Server**.
15. Click **Next** at the **Welcome to the Activate Server Wizard**.
16. Click **Next** at the **Connection Method** windows.
17. Click **Finished**, closing the **Activate Server Wizard**.
18. Close TS Licensing Manager.

---

#### **EXAM WARNING**

There may be licensing questions on the exam—Microsoft is stressing this more in the new exams. Remember, there are three ways to activate a Terminal Services License Server: Automatic Connection (Recommended), Web Browser, and Telephone.

---



## TEST DAY TIP

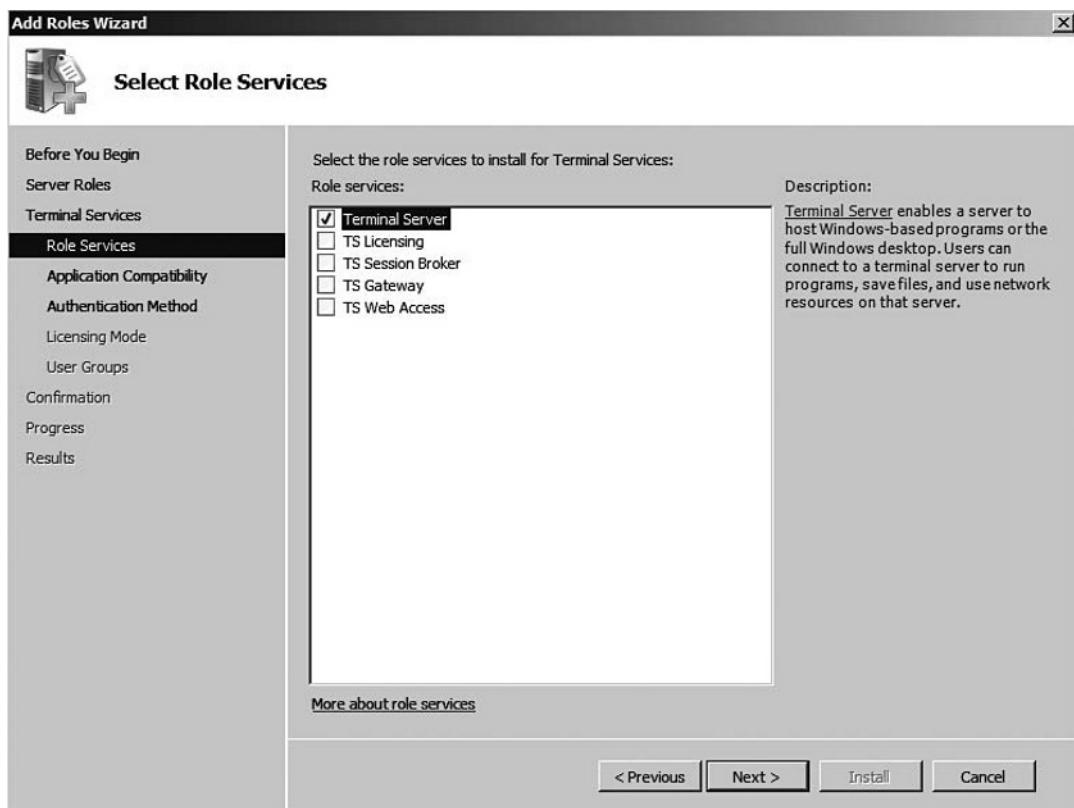
Microsoft gives you a 120-day grace period to install and activate your Microsoft Terminal Server licenses. After this 120 day period—clients will not be able to connect to the terminal server.

## EXERCISE 6.2

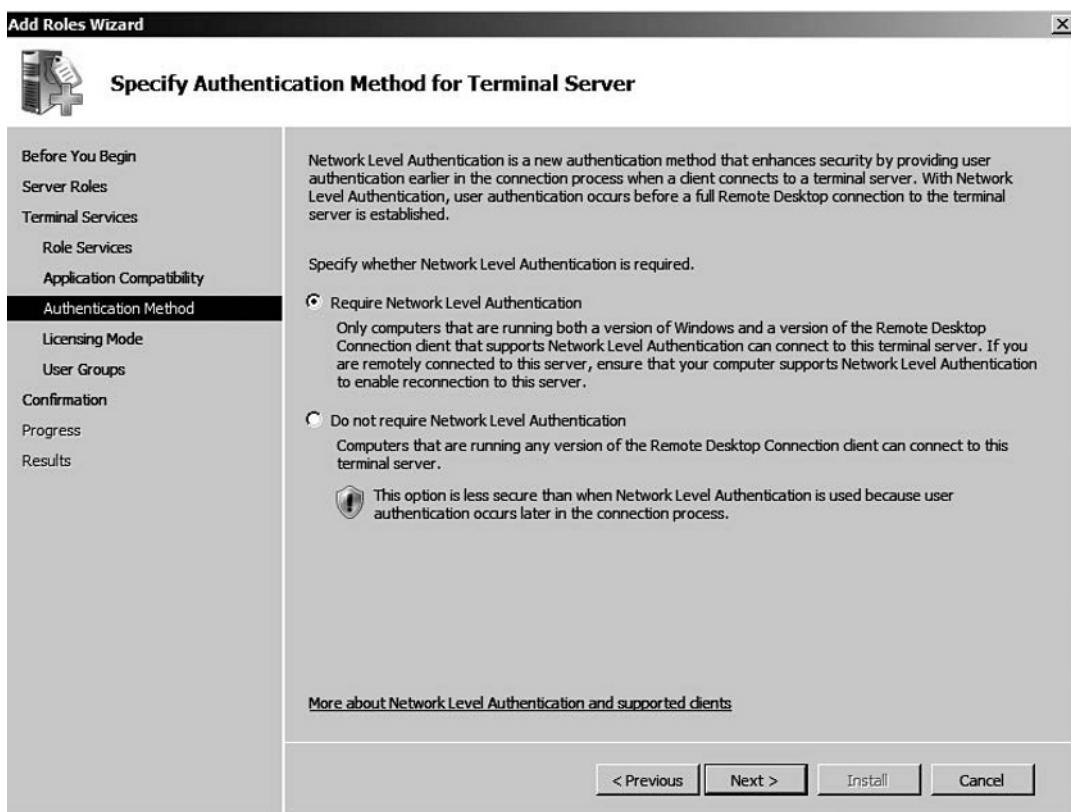
### INSTALL MICROSOFT WINDOWS 2008 SERVER TERMINAL SERVER

In this exercise, we are going to go ahead and install Terminal Server on TSSERVER02. We can do this now that we have a Terminal Service Licensing Server installed in our domain. The first few steps are the same as installing Terminal Licensing Server.

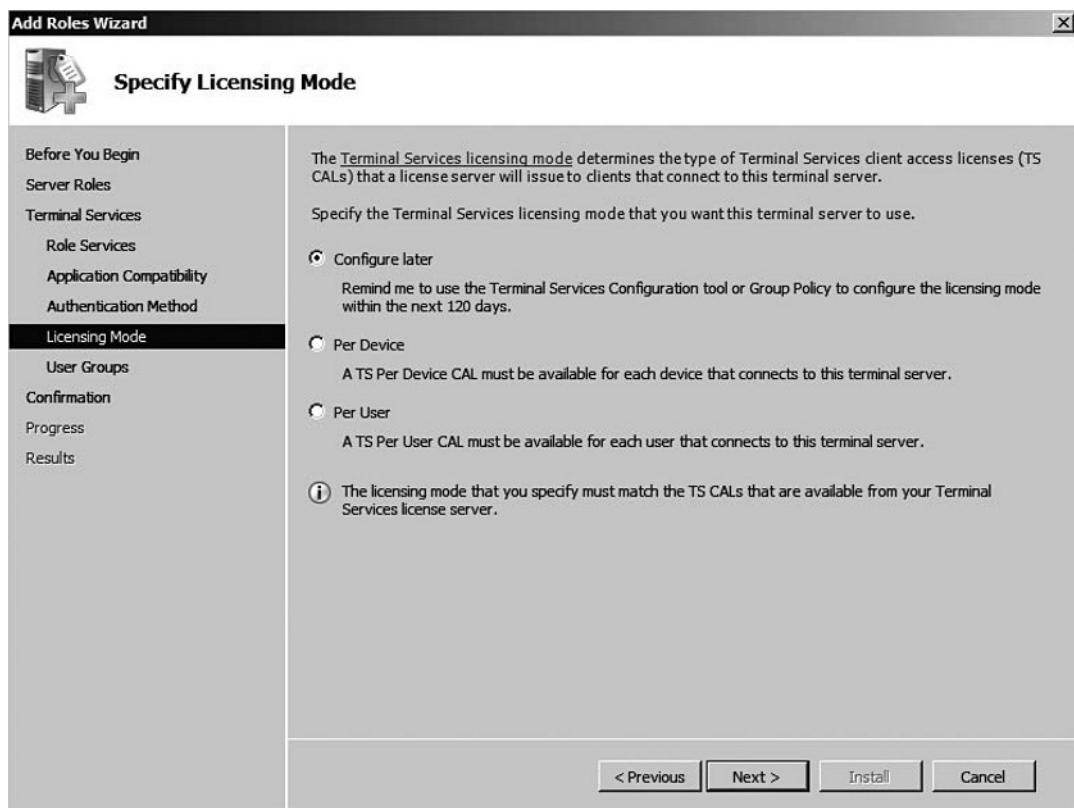
1. First, we will need to open the **Server Manager**. To do this, click on **Start** then **Server Manager** at the top of the Start Menu—refer back to Figure 6.2.
2. Within the Server Manager click **Roles**, and then click **Add Roles**.
3. At the next screen, click **Next** to continue.
4. Select the **Terminal Service** role and click **Next**. Refer back to Figure 6.3.
5. The next window is an **Introduction to Terminal Services**; click **Next**.
6. At the **Select Role Services** window, select **Terminal Server**—see Figure 6.6. Click **Next** to continue.

**Figure 6.6** Select Role Services

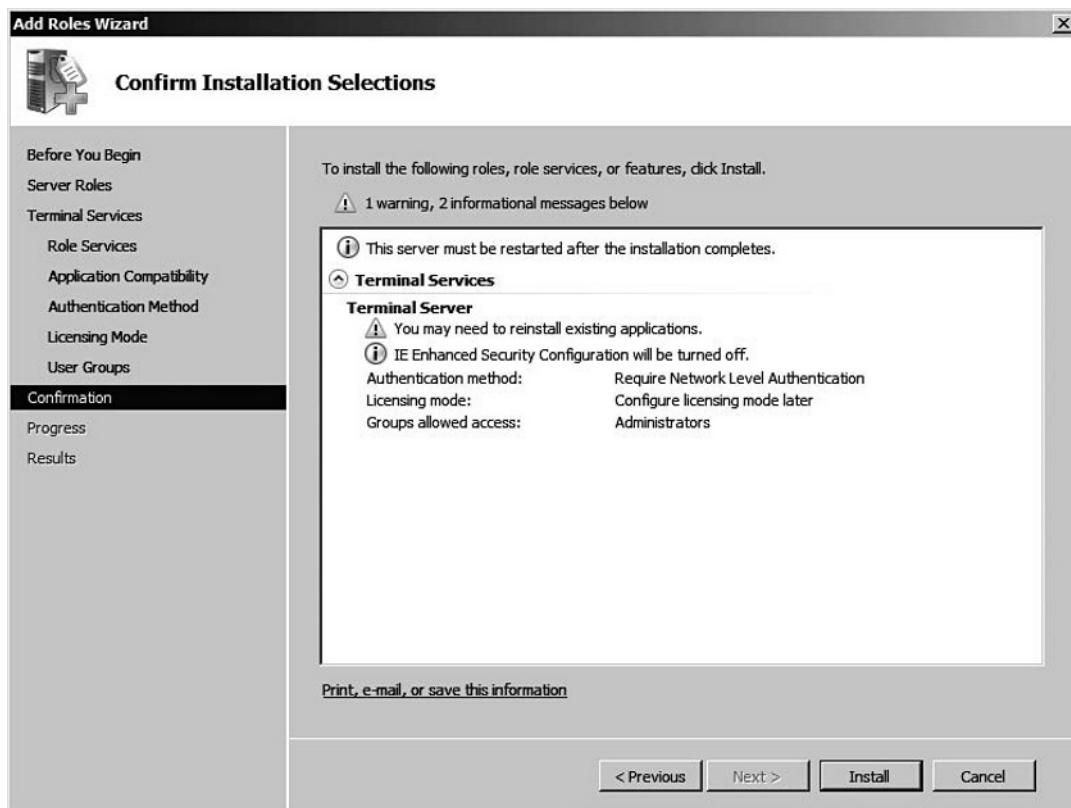
7. The next screen warns you to **Uninstall and Reinstall Applications for Compatibility**. Click **Next** to proceed. Note: This is very important. You do not want any applications you intend to make available to terminal server users installed before enabling terminal services on a server.
8. The next screen allows you to **Specify Authentication Method for Terminal Server**. Choose **Require Network Level Authentication**—see Figure 6.7. This choice is the most secured method of authentication for terminal servers. Click **Next** to continue.

**Figure 6.7** Specify Authentication Method for Terminal Server

9. The next screen, we need to **Specify Licensing Mode**. Since we do not have any licensing packs, choose **Configure later**—see Figure 6.8. Microsoft Windows 2008 Server gives you a 120 day grace period to install the actual licenses. Click **Next**.

**Figure 6.8** Specify Licensing Mode

10. We have to choose who has access to the terminal server in the **Select User Groups Allowed Access To This Terminal Server**. Accept the default setting for Administrators. Click **Next** to proceed.
11. **Confirm Installation Selections**—see Figure 6.9. Click **Install**.

**Figure 6.9** Confirm Installation Selections

12. The next screen warns that you need to restart the server. Click **Close**, then **OK** to restart the server.

### Configuring & Implementing...

#### RDP (3389) and NAT Firewalls

Before VPNs, both IPSec (Site to Site VPN Tunnels) and SSL (Microsoft Terminal Services Gateway Server), administrators would actually add a NAT statement to the firewall redirecting port 3389 to the internal terminal server. Then they would add an access rule to allow RDP traffic from the

Continued

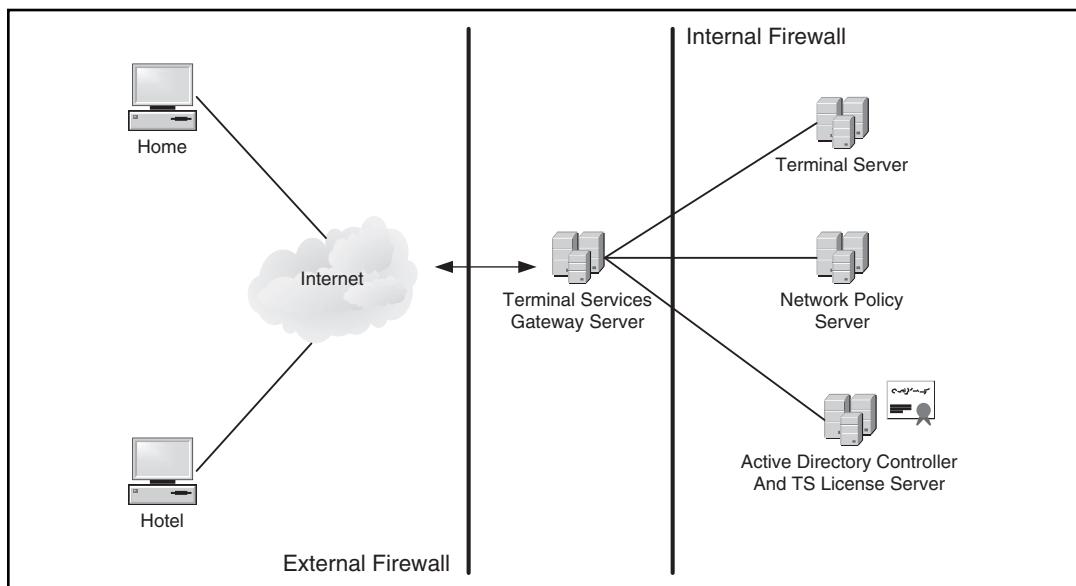
Internet side of the firewall into the terminal server. All you had to do at home was load Remote Desktop Connection (RDC) software and point it at the public IP address (or DHCP address from the ISP provider) and you were connected. Enter your credentials and you are in.

Though this is a very outrageous and unsecure method of connecting to the office place from outside the building—you would not believe the errors junior administrators do (such as this) to cause very unsafe computing practices. Usually they make this type of connection because it is simple and very effective in their untrained eyes—or should I say ineffective.

As a consultant to another IT person: Please take the time to secure your network properly. It will take a little longer to configure and you will need to probably contact someone for help or do some research—but please, take the time to do this job right! Your job may just be on the line!

## Terminal Services Gateway Server

Terminal Services Gateway Server allows for Remote Desktop Protocol (RDP) connections to securely connect over the Internet via the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) to terminal servers or internal network resources. This feature was first developed with connecting Microsoft Outlook to Exchange Servers via Remote Procedure Call over HTTPS. With Terminal Services Gateway Server, along with Network Access Protection (NAP), you can provide a comprehensive security configuration model that enables you to control access to specific internal network resources. Figure 6.10 depicts what an infrastructure layout may look like for Terminal Services Gateway Server.

**Figure 6.10 Terminal Services Gateway Server**

The clients outside the external firewall (public network) connect to the Terminal Services Gateway Server which contacts the resources behind the internal firewall (private network). RDP uses port 3389 to connect to a server directly for a terminal session. This type of connection was not suitable to use for connections over the Internet because most firewalls would block port 3389. Now that the RDP protocol is encapsulated into HTTPS and Secure Sockets Layer/Transport Layer Security (SSL/TLS)—it can easily transverse firewalls to setup a connection anywhere you have internet access. HTTPS uses a signed certificate to secure the connection between the client and private resource.

When installing the Terminal Services Gateway role to a Microsoft Windows 2008 Server, these other roles also must be installed (if these services are not installed, the Terminal Services Gateway role will install them automatically):

- Remote Procedure Call (RPC) over HTTP Proxy
- Internet Information Services (IIS) 7.0
- Network Policy and Access Services

## EXERCISE 6.3

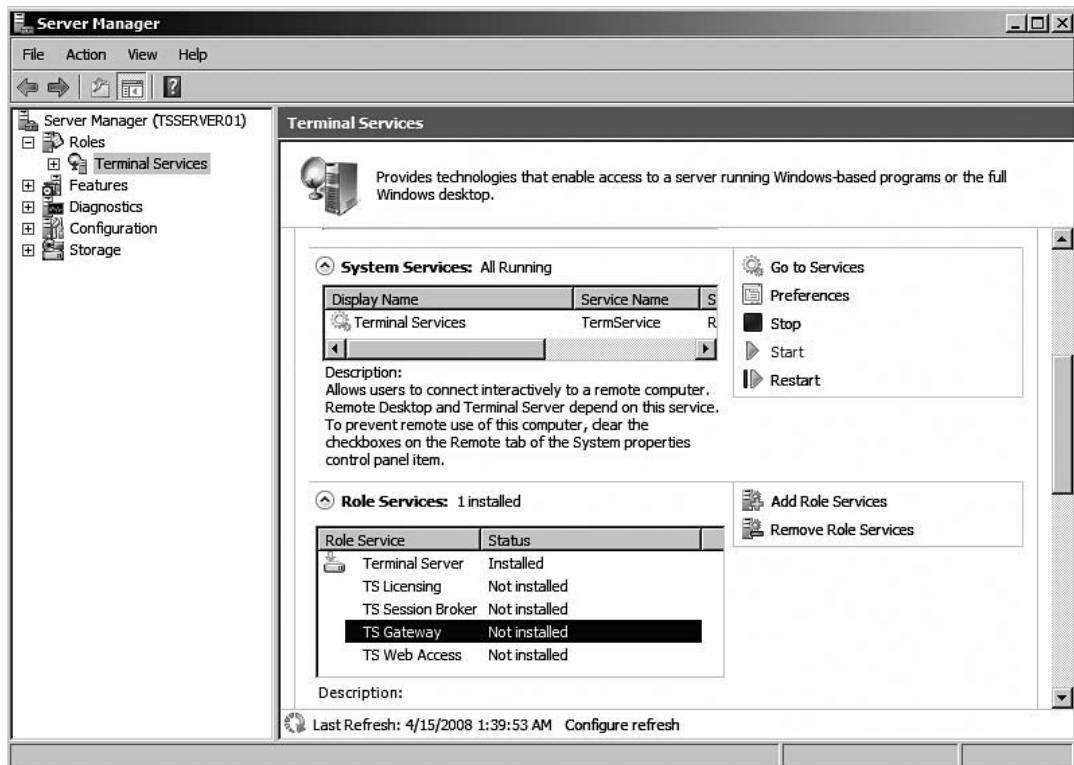
### INSTALLING MICROSOFT TERMINAL SERVICES GATEWAY

We are going to install the Microsoft Terminal Services Gateway on TSSERVER01 in this exercise. Since we already used the Roles Wizard in a preceding exercise, we will use the Server Manager to add the Microsoft Terminal Services Gateway. This will also illustrate an alternative way to do the installation.

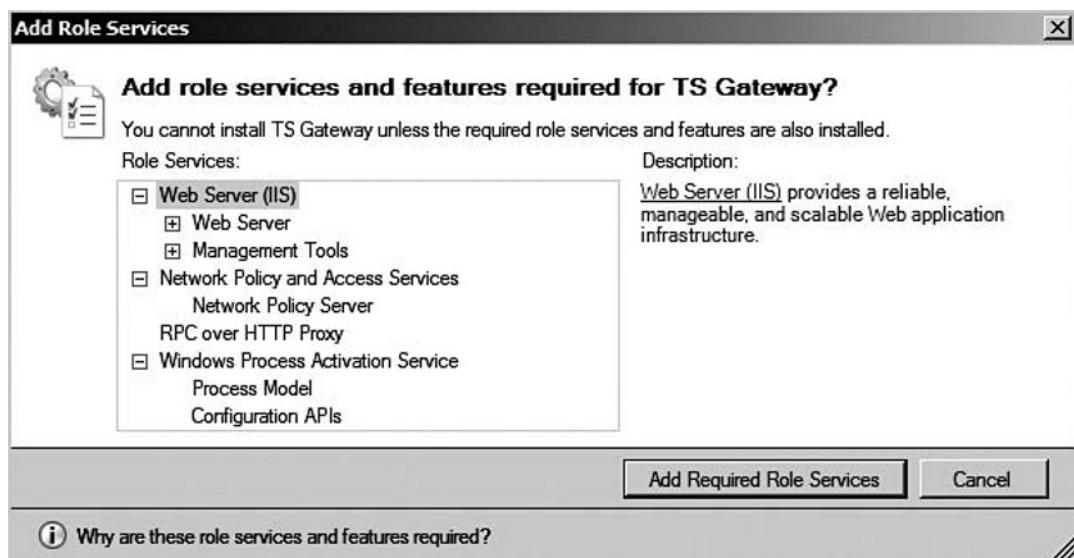
#### EXAM WARNING

On the exam, you will be given scenario questions. Some of the scenario questions will only make a particular option available to do an installation. It is important to know how to install Roles from the Roles Wizard and from within the Server Manager.

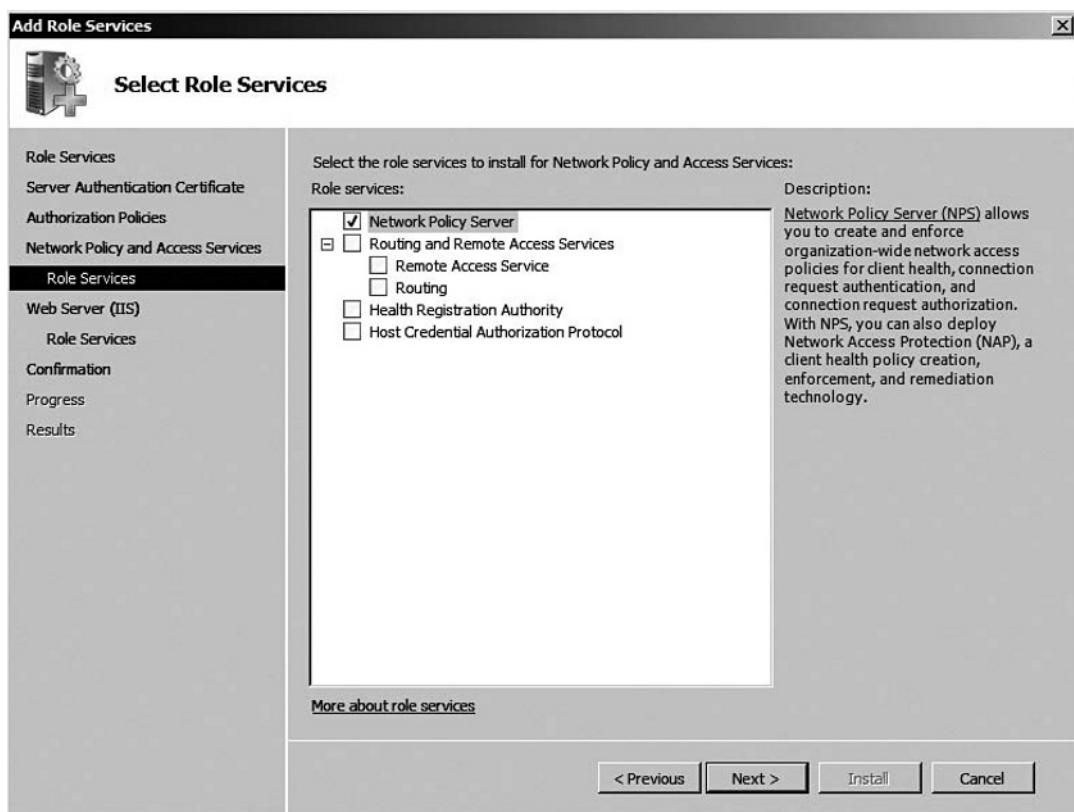
1. First, we will need to open the **Server Manager**. To do this, click on **Start** then **Server Manager** at the top of the Start Menu—refer back to Figure 6.2.
2. Expand **Roles**, then select **Terminal Services**—see Figure 6.11. Scroll the right pane windows down to where you can see **Roles Services**.

**Figure 6.11** Server Manager

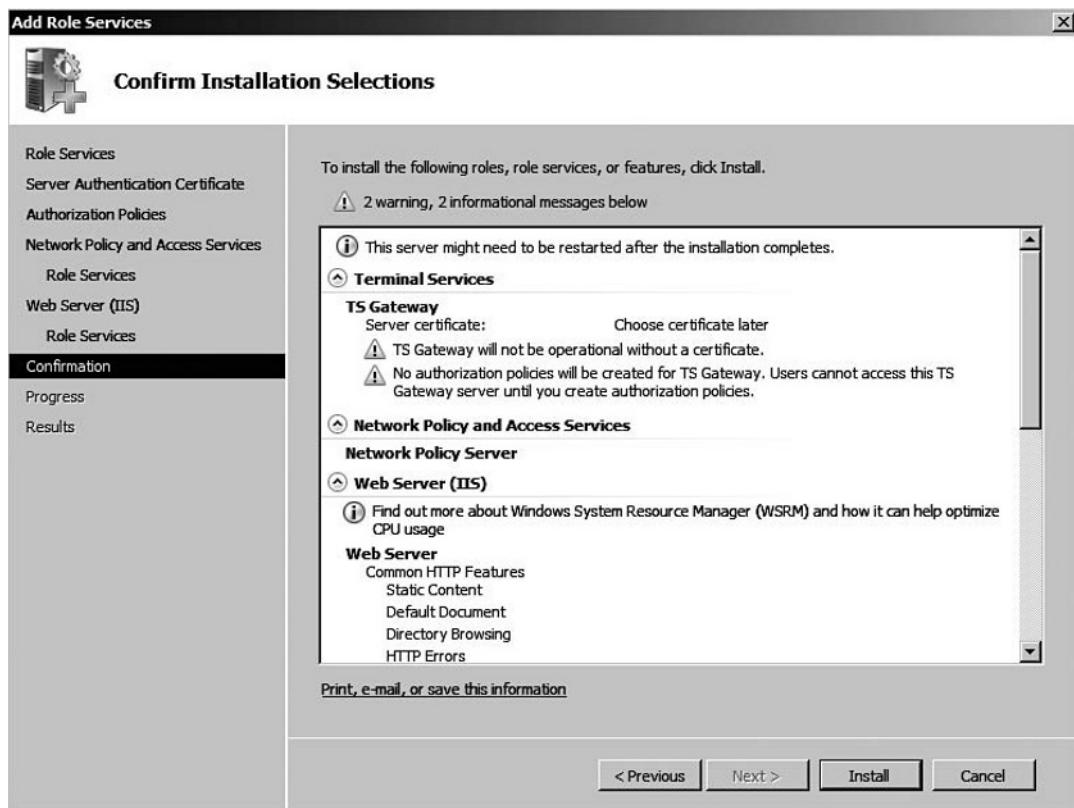
3. Select the **TS Gateway** and click **Add Role Services**.
4. The **Add Role Services** window is displayed. Select **TS Gateway** and click **Next**.
5. The **Add role services and features required for TS Gateway** is displayed—see Figure 6.12. Click **Add Required Role Services**.

**Figure 6.12** Add Role Services and Features Required for TS Gateway

6. Click **Next** to continue.
7. The next window is the **Choose a Server Authentication Certificate for SSL Encryption**. Since we have no certificate, select **Choose a certificate for SSL encryption later**. Click **Next**.
8. The **Create Authorization Policies for TS Gateway** is the next window. Select **Later** and click **Next**.
9. Click **Next** at the **Network Policy and Access Services** screen.
10. Verify that the **Network Policy Server** is checked in the window. See Figure 6.13. Click **Next** to continue.

**Figure 6.13** Select Role Services

11. The **Web Server (IIS)** window is shown. Click **Next** to continue.
12. In the **Select Role Services**, Windows has already selected all of the IIS components necessary to install Terminal Services Gateway. Click **Next** to continue.
13. You are presented with a **Confirm Installation Selections**. Verify your selections—see Figure 6.14. Click **Install**.

**Figure 6.14** Confirm Installation Selections

14. Verify the installation completed successfully and click **Close** to return to the **Server Manager**.
15. Click **File**, and then **Exit** to close the **Server Manager**.

## Terminal Services Session Broker

In Windows Server 2003, Microsoft revealed a new feature for Terminal Services to allow administrators to load balance Terminal Services sessions and reconnect disconnected sessions. Microsoft Windows 2008 Server builds on this idea and renamed it the Terminal Server Session Broker.

Terminal Services Session Broker (TS Session Broker) is reintroduced to Microsoft Windows 2008 Server as a server role. Basically, the TS Session Broker allows you to enable a user to reconnect to an existing session in a load-balanced terminal server farm, and probably more important, the TS Session Broker enables you as an administrator to distribute the session load between servers in a load-balanced server farm. There are some special considerations to make the TS Session Broker work as expected:

- To participate in a TS Session Broker Load Balancing—the TS Session Broker and terminal servers in the farm must be running Microsoft Windows 2008 Server. The TS Session Broker role is available in Microsoft Windows 2008 Server Standard Edition, Microsoft Windows 2008 Server Enterprise Edition, and Microsoft Windows 2008 Server Datacenter Edition. Microsoft Windows 2003 Servers cannot use the TS Session Broker Load Balancing feature.
- Clients must be using the Remote Desktop Connection (RDC) version 5.3 or later to use the TS Session Broker Load Balancing feature.

### Configuring & Implementing...

#### How Does this Load-Balancing Work?

It comes up often—how does the TS Session Broker perform load-balancing? There are two major steps when a user connects to a Terminal Server Farm:

The user connects to the server farm by a preliminary load-balancing mechanism. After the user connects, the accepting terminal server then queries the TS Session Broker server to determine where to redirect the user.

Continued

The accepting terminal server redirects the user to the specified server from the TS Session Broker. The TS Session Broker will either connect a user to a server where the user has a disconnected session, or the TS Session Broker will connect to the terminal server that has the fewest sessions.

The interesting statement is “a preliminary load-balancing mechanism”. Basically, before even the TS Session Broker gets involved in the connection—the initial load-balancing has occurred. The easiest load-balancing mechanism to deploy is DNS Round Robin. The other potential Microsoft technology to perform the initial load-balancing includes Windows Network Load Balancing (NLB).

The other option for load-balancing would be a hardware option. Hardware options would include: Citrix Netscaler, Barracuda Load Balancer, or F5 Networks BIG-IP Local Traffic Manager (there are also countless other vendors in this market—this is just a sample).

### EXAM WARNING

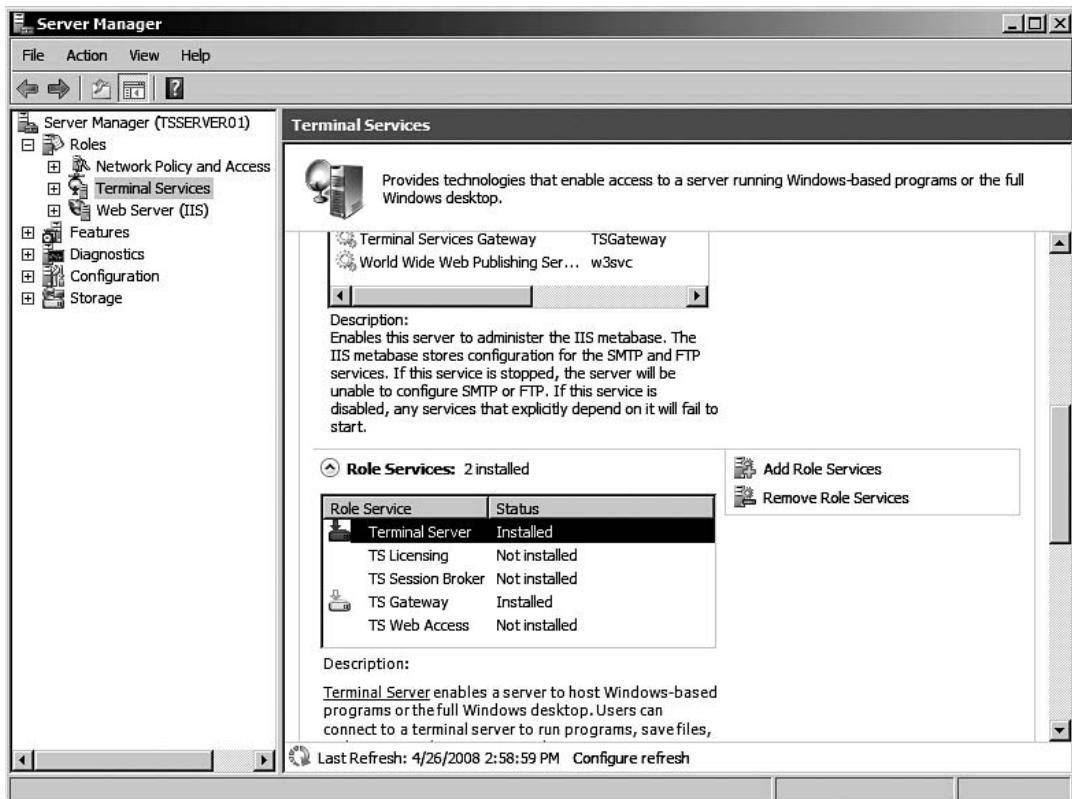
The only type of load-balancing you need to concern yourself with on the exam would be DNS Round Robin and Microsoft Windows Network Load Balancing (NLB).

## EXERCISE 6.4

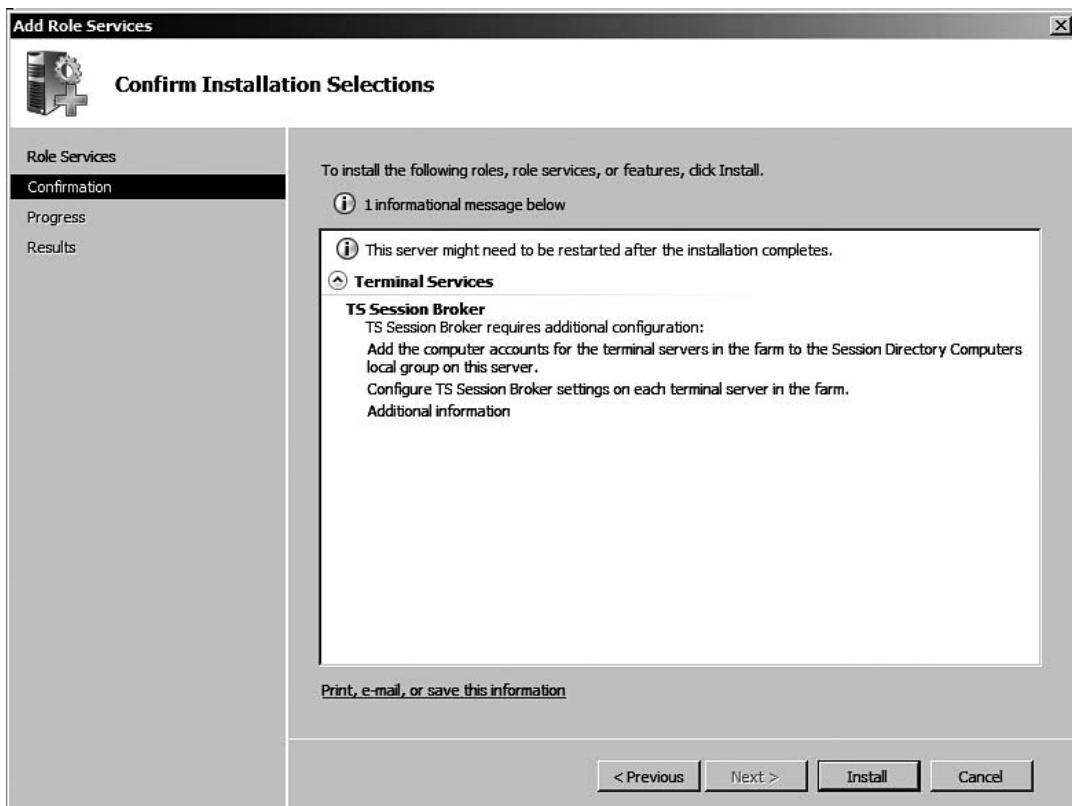
### INSTALLING MICROSOFT TERMINAL SERVICES SESSION BROKER

In this exercise, we are going to install the Microsoft TS Session Broker on the TSSERVER01 terminal server that we have worked with in previous exercises.

1. First, we will need to open the **Server Manager**. To do this, click on **Start** then **Server Manager** at the top of the Start Menu—refer back to Figure 6.2.
2. Expand **Roles**, and then select **Terminal Services**. Scroll the right pane windows down to where you can see **Roles Services** and click **Add Role Services**—see Figure 6.15.

**Figure 6.15** Server Manager

3. Select **TS Session Broker** and click **Next**.
4. Click **Install** at the **Confirm Installation Selections** window—see Figure 6.16.

**Figure 6.16** Confirm Installation Selections

5. At the **Add Role Services** windows, click **Close**.
  6. Click **File**, and then **Exit** to close the **Server Manager**.
-

## Terminal Services RemoteApp

Microsoft Terminal Services RemoteApp allows an administrator to publish applications to a user in a window that looks as if the application is running locally on the clients' computer. If you are familiar with Citrix XenApp—this would be the equivalent to a seamless window. A user can minimize, maximize and resize the program window—you can also start numerous RemoteApps on a client. TS RemoteApp is compatible with the following operating systems:

- Microsoft Windows Vista
- Microsoft Windows 2008 Server
- Microsoft Windows XP Service Pack 2 with the new Remote Desktop Connection (RDC) Client
- Microsoft Windows 2003 Server Service Pack 1 with the new Remote Desktop Connection (RDC) Client

RemoteApp is a very powerful feature for administrators. Not only is the ability to run terminal service applications seamlessly important—but sending users the configurations and pushing it down to clients can be done in a number of ways which lends itself to being a solution to many connection issues. The files used in conjunction with RemoteApp that contain the settings include RDP files for the Remote Desktop Connection (RDC) and Windows Installer Packages. Users can run RemoteApp programs in the following ways:

- Double-click a Remote Desktop Protocol (RDP) file that has been created and distributed by the administrator.
- Double-click a program icon on their desktop or **Start** menu that has been created and distributed by the administrator with a Windows Installer (MSI) Package.
- Double-click a file whose extension is associated with a RemoteApp program.
- Access a link to the RemoteApp program on a Web site by using Microsoft Terminal Service Web Access.

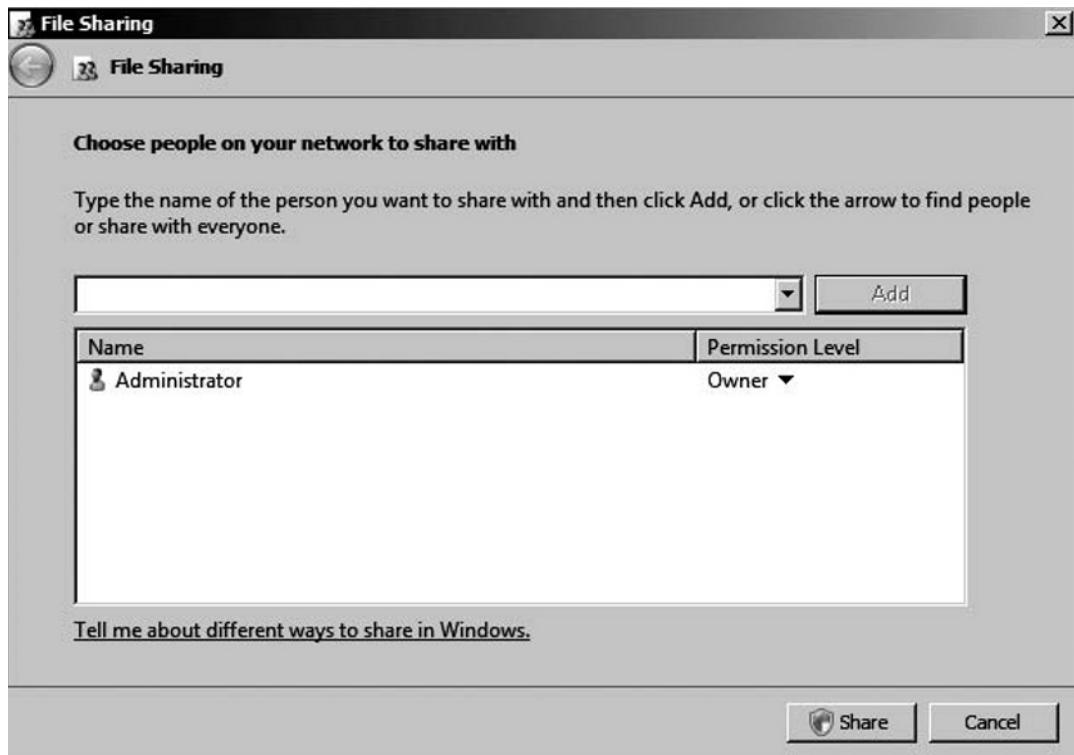
## EXERCISE 6.5

### INSTALLING A REMOTEAPP FROM A WINDOWS INSTALLER PACKAGE

In this exercise, we are going to use RemoteApp to build a Windows Installer Package and distribute it via a file share. We will be deploying Microsoft Windows 2008 Server Manager to a Windows Vista client via a file share. You will need to use the TSSERVER01 and a Windows Vista client with network access to the TSSERVER01 terminal server.

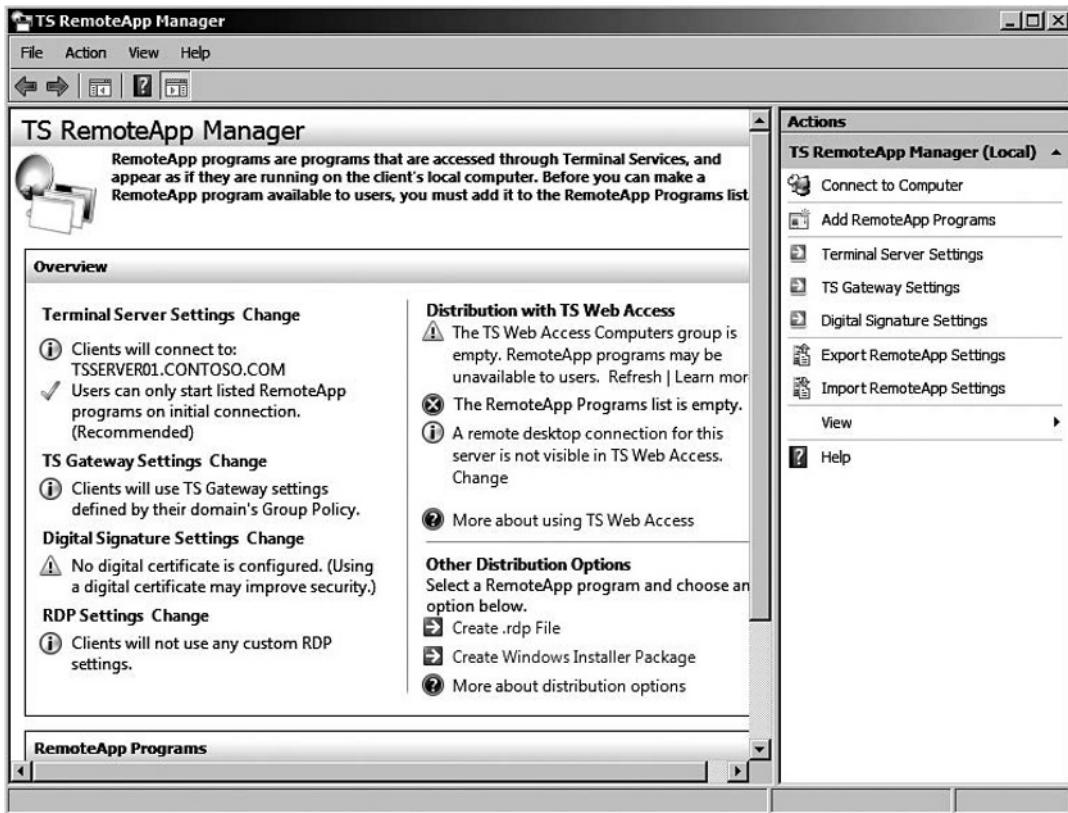
1. On the TSSERVER01, click **Start** and then **Computer**.
2. Double-click **Local Disk (C:)**.
3. Right-click and choose **New**, and then **Folder**. Name the new folder **RemoteApp**.
4. Right-click the **RemoteApp** folder and choose **Share**.
5. Click **Share** at the **File Sharing** window (see Figure 6.17).

**Figure 6.17** File Sharing

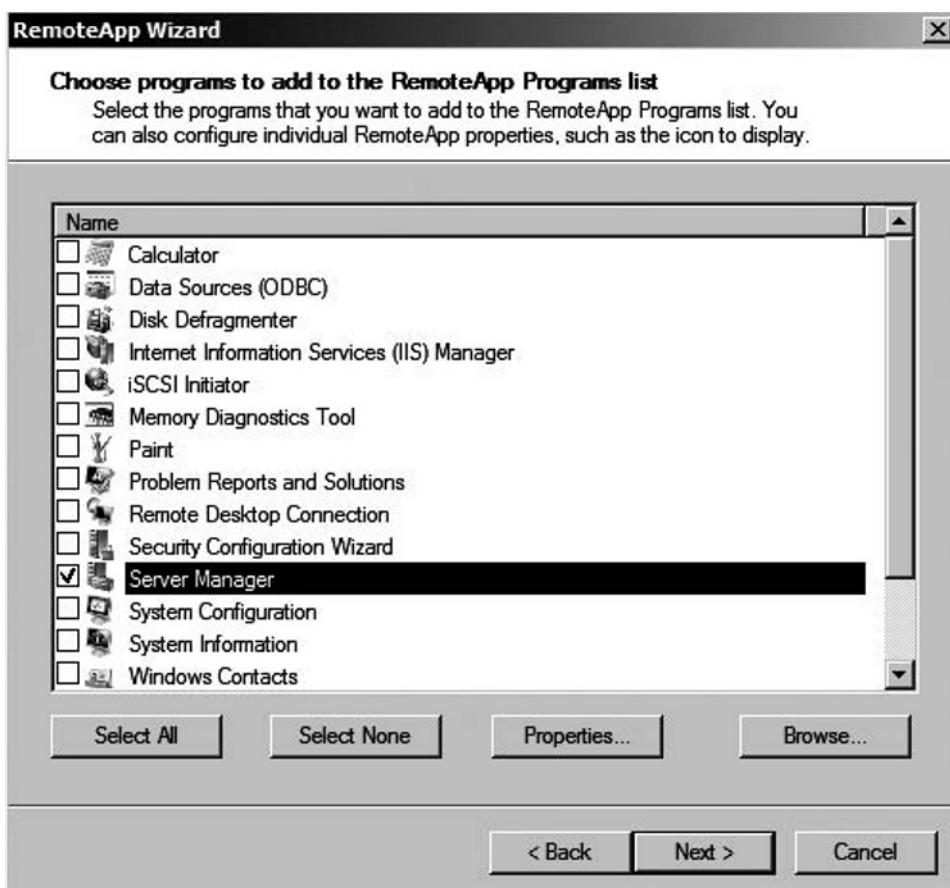


6. Click Done at the File Sharing window.
7. Click Start | Administrative Tools | Terminal Services | TS RemoteApp Manager. See Figure 6.18.

**Figure 6.18** TS RemoteApp Manager

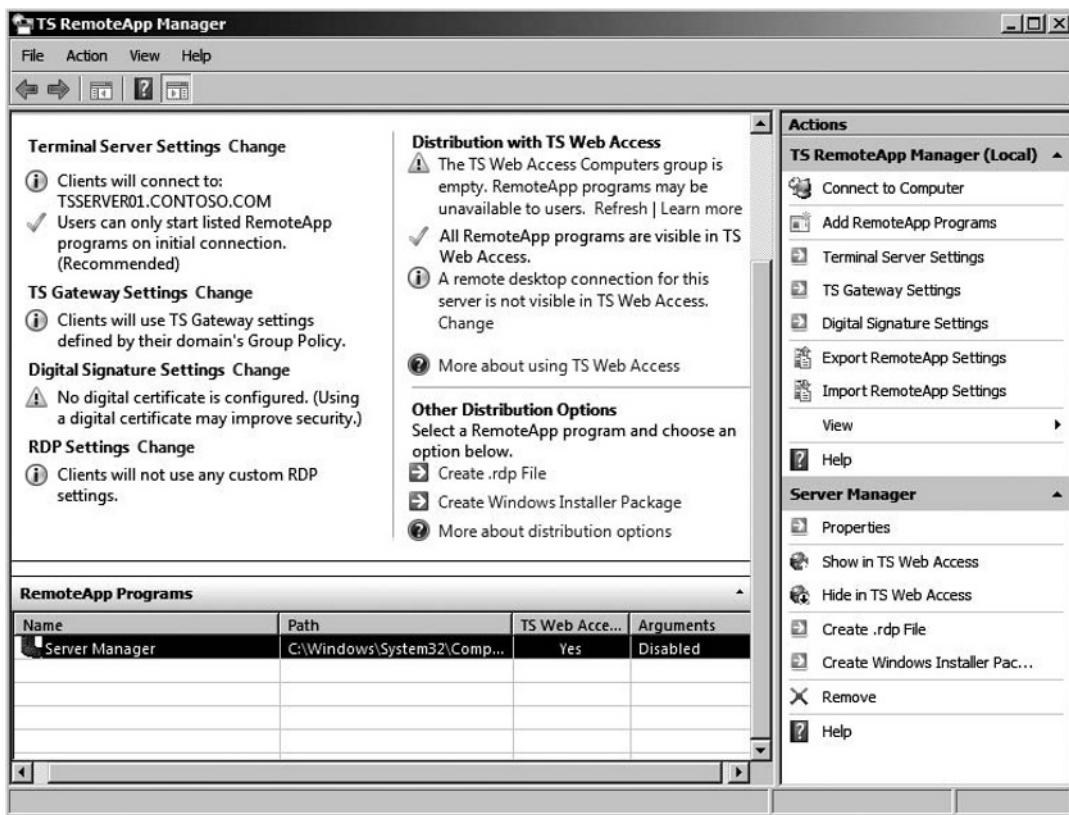


8. In the right pane of the **TS RemoteApp Manager**, click **Add RemoteApp Programs**.
9. Click **Next** in the **Welcome to the RemoteApp Wizard**.
10. At the next window, **Choose programs to add to the RemoteApp Programs list**, select **Server Manager** and then click **Next**. See Figure 6.19.

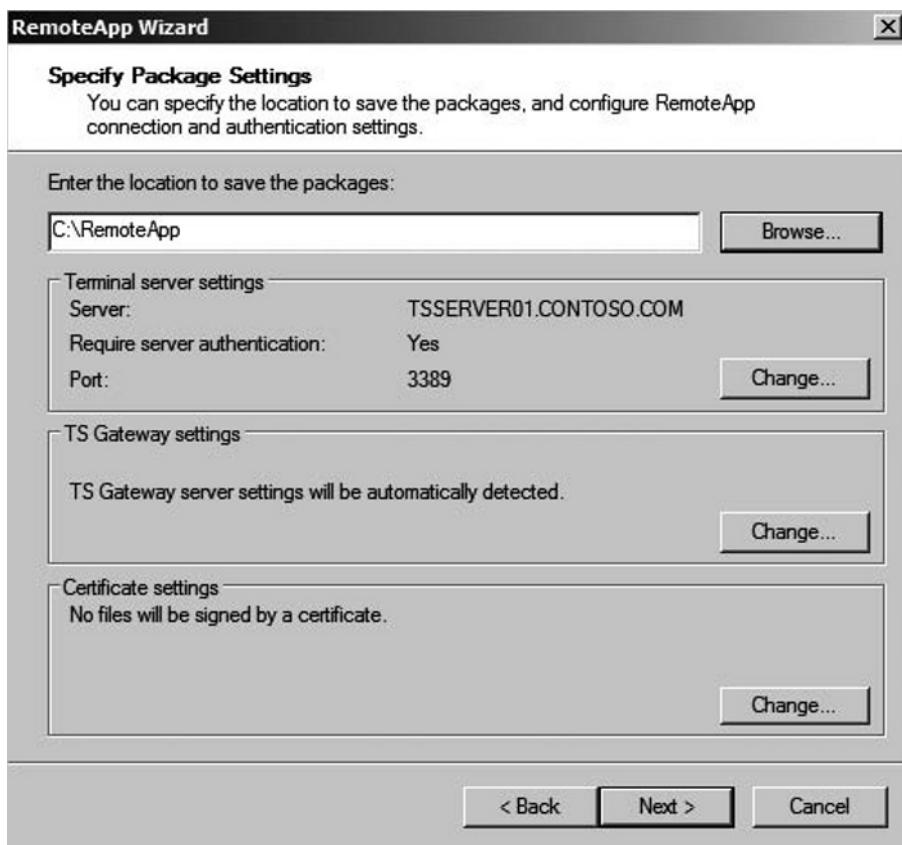
**Figure 6.19** RemoteApp Wizard

11. In the **Review Settings** window, click **Finish**.
12. At the **TS RemoteApp Manager**, select **Server Manager** from the **RemoteApp Programs**. See Figure 6.20. Select **Create Windows Installer Package**.

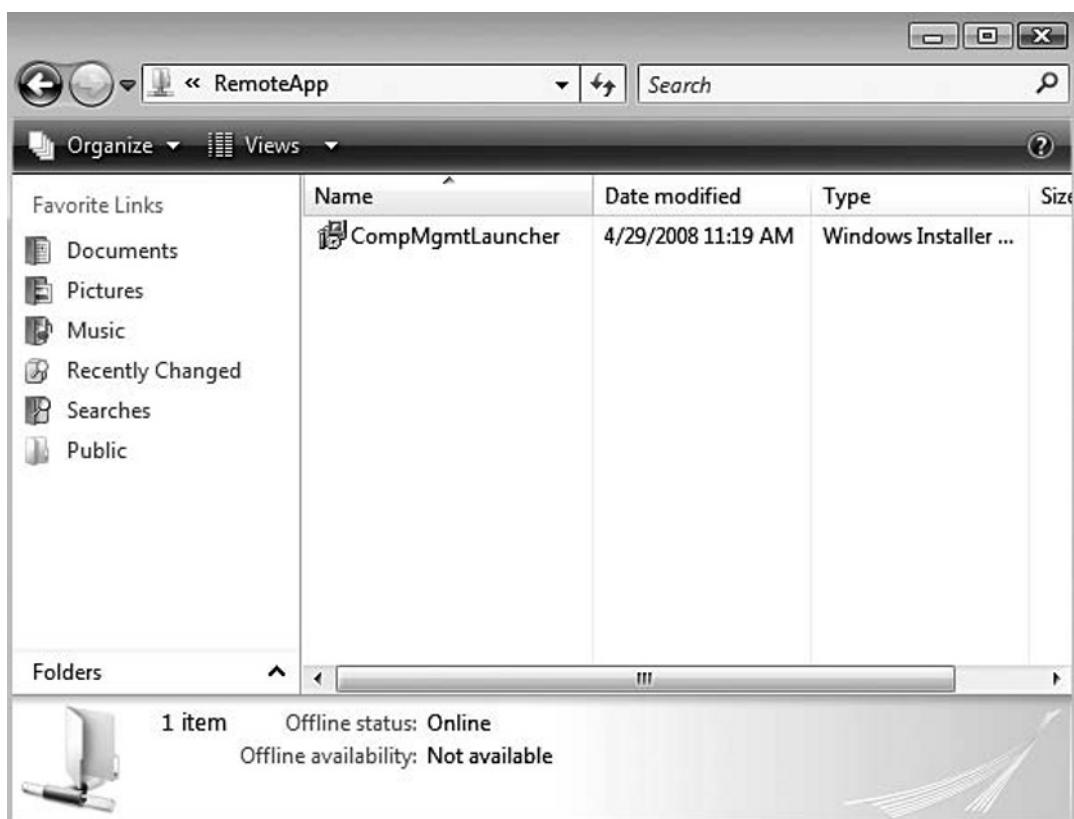
**Figure 6.20 TS RemoteApp Manager**



13. In the **Welcome to the RemoteApp Wizard**, click **Next**.
14. In the **Specify Package Settings**, click **Browse** and select the folder you created earlier, C:\RemoteApp. Your settings should look like Figure 6.21. Click **Next** to continue.

**Figure 6.21** Specify Package Settings

15. At the next windows, **Configure Distribution Package**, select **Desktop** to put an icon on the user's desktop for Server Manager. Click **Next**.
16. In the **Review Settings** window, click **Finish**.
17. Log on as Administrator into your Microsoft Windows Vista client. **This exercise assumes that the Windows Vista client is a member of the CONTOSO.COM domain.**
18. Click **Start** and clear **Start Search**. Type **\TSSERVER01\REMOTEAPP** and push **Enter**. This will bring up the share you created on TSSERVER01 for the RemoteApp Server Manager installer. See Figure 6.22.

**Figure 6.22** RemoteApp Share on TSSERVER01

19. Double-click **CompMgmtLauncher.MSI** to start installation.
20. After the installation completes, you will have a **Server Manager** icon on the desktop and in the Start Menu.
21. Double-click **Server Manager** and click **Continue** at the **The publisher of this remote connection cannot be identified** prompt.
22. Log in as Administrator in the domain.
23. The Server Manager will start.

---

## Resource Allocation

One of the biggest concerns to a Windows network administrator, especially in a Terminal Services environment, is managing computing resources and making sure that no one process or user consumes all of these computing resources. Managing your resources can help ensure that all of the services provided by a single server are

available on an equal basis or that your resources will always be available to high-priority applications, services, or users. In Microsoft Windows Server 2008 Enterprise Edition, Microsoft has made the Microsoft Windows System Resource Manager available to help administrators with this often complicated task.

## Microsoft Windows System Resource Manager

Administrators can use Microsoft Windows System Resource Manager to manage server processor and memory usage with standard built-in or custom resource policies. The four built-in policies allow for an administrator to quickly implement Microsoft Windows System Resource Manager without any additional configuration—this will save you a lot of time and experimenting. The four built-in resource management policies are displayed in Table 6.1.

### TEST DAY TIP

Microsoft Windows System Resource Manager will only manage processor resources once the total combined processor resources are greater than 70% of available processor resources.

**Table 6.1** Built-in Resource Management Policies

Policy	Description
Equal Per Process	When the <b>Equal_Per_Process</b> resource allocation policy is managing the system, each running process is given equal treatment. For instance, if a server reaches 70% processor utilization—this policy will give each process an equal amount of processor utilization.
Equal Per User	When the <b>Equal_Per_User</b> resource allocation policy is managing the system, processes are grouped according to the user account that is running them and each of these process groups is given equal treatment. For example, if four users are running processes on the server, each user will be allocated 25% of the system resources to complete those processes. A user running a single application is allocated the same resources as a user running several applications. This policy is useful for application servers. Examples of applications servers would be those using Internet Information Server (IIS) or ASP.NET.

Continued

**Table 6.1 Continued.** Built-in Resource Management Policies

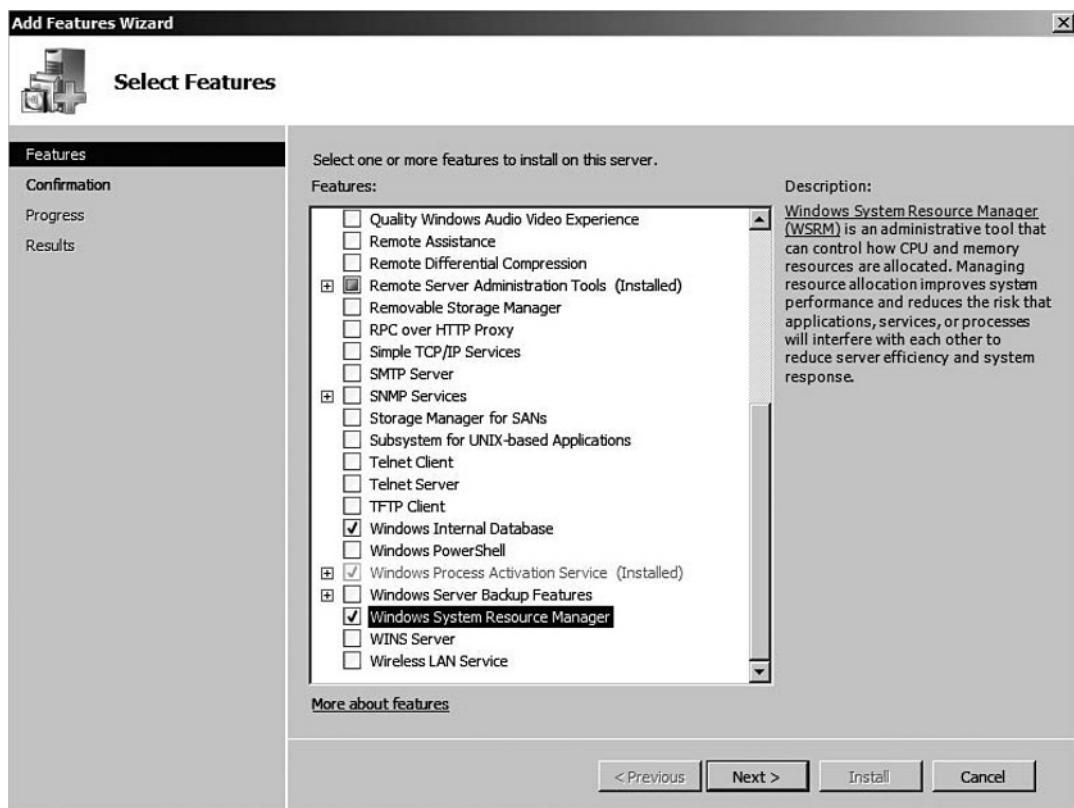
Equal Per Session	When the <b>Equal_Per_Session</b> resource allocation policy is managing the system, resources are allocated on an equal basis for each connected session. This is the policy that would be typically enforced with the roll out of terminal servers.
Equal Per IIS Application Pool	When the <b>Equal_Per_IISAppPool</b> resource allocation policy is managing the system, each running IIS application pool is given equal treatment, and applications that are not in an IIS application pool can only use resources that are not being consumed by IIS application pools.

## EXERCISE 6.6

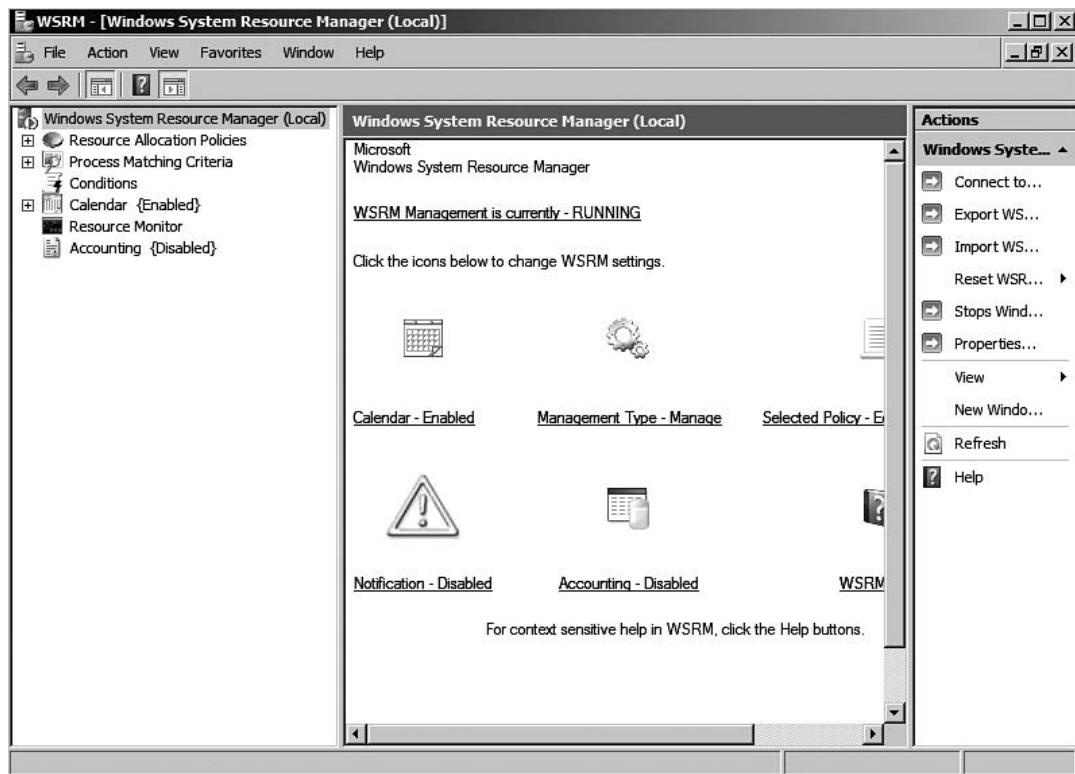
### INSTALL MICROSOFT WINDOWS SYSTEM RESOURCE MANAGER AND APPLY THE EQUAL\_PER\_SESSION POLICY

In this exercise, we are going to install the Microsoft Windows System Resource Manager and apply the Equal\_Per\_Session built in resource management policy to our terminal server—TSSERVER01. Your terminal server (TSSERVER01) will need to be running Microsoft Windows 2008 Server Enterprise Edition to perform this exercise.

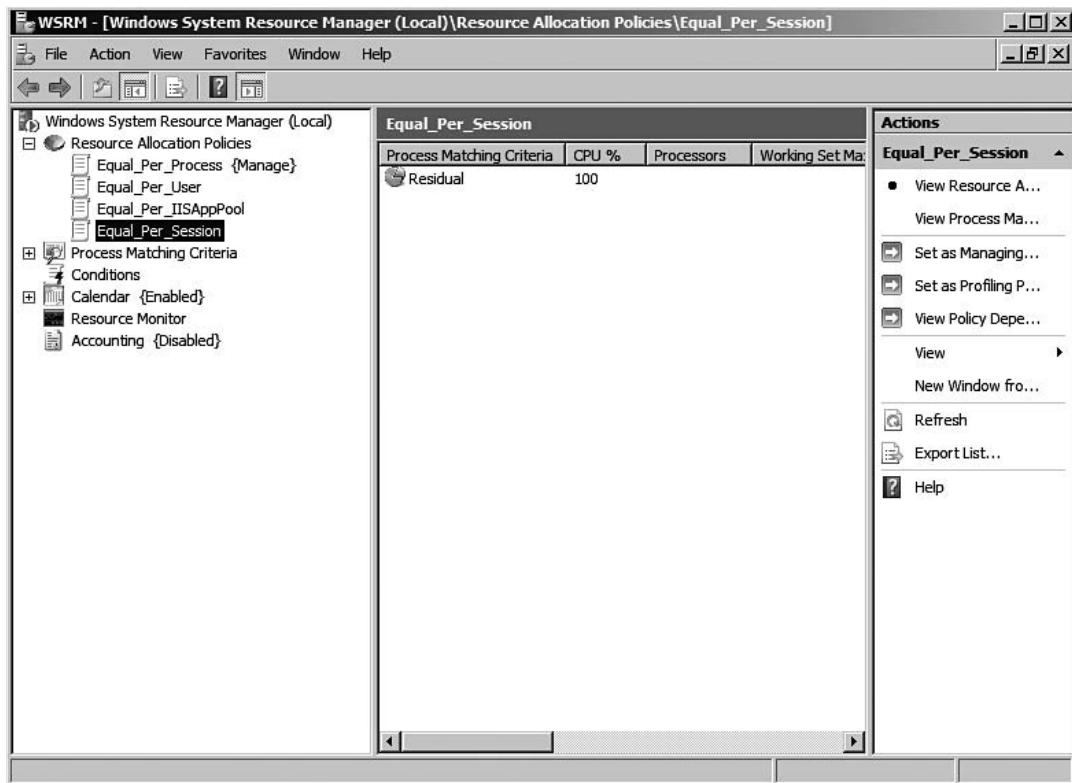
1. Click **Start** and open **Server Manager**.
2. Click **Features** in the left pane tree and then click **Add Features** in the right pane.
3. In the **Add Features Wizard**, select **Windows System Resource Manager**. When prompted to **Add Required Features** click **Add Required Features**. See Figure 6.23.

**Figure 6.23** Add Features Wizard

4. Click **Next**.
5. In the **Confirm Installation Selections**, click **Install**.
6. When the **Installation Results** window come up, verify that all installations where successful. Click **Close** to finish the installation.
7. Click **File** then **Exit** to close the **Server Manager**.
8. Click **Start | Administrative Tools | Windows System Resource Manager**. When prompted to **Connect to computer** choose **This computer** and click **Connect**. The Windows System Resource Manager Windows should look like Figure 6.24.

**Figure 6.24** Windows System Resource Manager

9. Expand **Resource Allocation Policies** and then select **Equal\_Per\_Session**. See Figure 6.25.

**Figure 6.25** Resource Allocation Policies

10. Right-click **Equal\_Per\_Session** and click **Set as Managing Policy**. Click **OK** to the warning box concerning the calendar. Microsoft Windows System Resource Manager has now applied the **Equal\_Per\_Session** resource allocation policy.
11. Click **File** and then **Exit** to close the Microsoft Windows System Resource Manager.

---

## Application Virtualization

Microsoft Virtualization sometimes gets confused with Microsoft Terminal Services—they can actually work together in some cases. Microsoft Virtualization can be managed by Microsoft System Center. The four products and their virtualization roles in the Microsoft Virtualization line of products include:

- Microsoft Terminal Services—Presentation Virtualization
- Microsoft Virtual Server 2005 R2—Server Virtualization

- Microsoft Virtual PC 2007—Desktop Virtualization
- Microsoft SoftGrid—Application Virtualization

## Microsoft SoftGrid Application Virtualization

Microsoft has joined the application virtualization market a leader after the purchase of Softricity. The main component for the Microsoft application virtualization platform is Microsoft SoftGrid Application Virtualization. In this section, we are going to look over the features and the overall platform of Microsoft SoftGrid Application Virtualization—however, there will be no exercises. The exam this book covers will not ask for configuration information and the topic alone could span its own text.

Microsoft SoftGrid Application Virtualization transforms applications into virtualized, network available services resulting in dynamic delivery of software that is never installed and never conflicts with other applications. For example: imagine being able to run Microsoft Office 97, Microsoft Office 2000 and Microsoft Office 2007—with Microsoft SoftGrid, this is easily accomplished without installing the application on the actual client. The programs are made available when needed and streamed to the client computer—but never installed on the client computer. These streamed applications do use the resources of the client computer—but never physically remain installed on the client computer. The applications do not get installed or altered after the operating system. The files streamed during the client include:

- Files (Including System Files)
- Registry
- Fonts
- Application INI Files
- COM/DCOM Objects
- Services
- Name Spaces

### **EXAM WARNING**

On this exam, you will not be expected to know how to administer Microsoft SoftGrid Application Virtualization.

# System Center Configuration Manager 2007

Microsoft System Center Configuration Manager 2007 was born from Microsoft System Management Server 2003. Microsoft System Configuration Manager 2007 provides monitoring along with configuration for software and hardware in a Microsoft platform environment. The important features of Microsoft System Center Configuration Manager 2007 include:

- Hardware and software inventory.
- Distributing and installing software applications.
- Distributing and installing updates to software, for example security fixes. This includes both Microsoft and third party applications.
- Works with Windows Server 2008 operating system Network Policy Server (NPS) to restrict computers from accessing the network if they do not meet specified requirements and providing remediation services to the client being denied access.
- Operating system deployment.
- Specifying what a desired configuration would be for one or more computers and then monitoring adherence to that configuration.
- Metering software usage for licensing compliance.
- Remotely controlling computers to provide troubleshooting support.

In the next several sections, we are going to explore Microsoft System Center Configuration Manager 2007.

## EXAM WARNING

Although the product name has officially changed to System Center Configuration Manager 2007, there are some programmatic elements within System Center Configuration Manager 2007 that have not been changed to reflect the new name. For example, the provider is still called the SMS Provider because changing it would have created backward compatibility problems for customers using WMI scripting. Many status messages still refer to SMS because the messages could apply to an SMS 2003 child site. Services, file names, shared folder names, and System Center Configuration Manager 2007 groups still retain the SMS abbreviation in their names.

## Introduction to SCCM

Microsoft System Center Configuration Manager 2007 allows you to perform and automate many administrative tasks—as listed above. But, the most basic level of a Microsoft System Center Configuration Manager 2007 configuration is the site. A site is basically a way to group clients into manageable units with similar requirements for feature sets, bandwidth, connectivity, language, and security. Microsoft System Center Configuration Manager 2007 sites can match your Active Directory sites or implementation—but, this is not a requirement. Microsoft System Center Configuration Manager 2007 sites can be totally different from the AD design. Clients can move between sites or even be managed from remote locations like home offices.

The actual installation of Microsoft System Center Configuration Manager 2007 is somewhat complicated and out of the scope of this book. We will be looking at the Microsoft Systems Center Configuration Manager 2007 Management Console and how to perform certain tasks. You can (and should) install the trial version of Microsoft System Center Configuration Manager 2007 onto your test network. A simple single site, single server installation is pretty straightforward—as long as all of the prerequisites are installed. Here is a list of the prerequisites:

- All site servers must be a member of a Windows 2000, Windows 2003 or Windows 2008 Active Directory domain.
- Background Intelligent Transfer Service (BITS) installed. This service is not installed by default in Microsoft Windows 2008 Server and will need to be enabled manually from within Server Manager.
- Internet Information Services (IIS) 6.0 or later.
- On Microsoft Windows 2008 Server—WebDAV extensions. WebDAV extensions were not released with the Microsoft Windows 2008 Server release to manufacturing. They will need to be downloaded here: <http://www.microsoft.com/downloads/details.aspx?familyid=036269FA-0040-4CCD-AD3D-78DA1EE132FB&displaylang=en>.
- Microsoft Management Console (MMC) 3.0
- .Net Framework 2.0
- Microsoft SQL Server 2005 Service Pack 2, Microsoft SQL Server Express Edition is not supported.



## TEST DAY TIP

---

Microsoft SQL Server 2005 Service Pack 2 is now required to host the site database. Microsoft SQL Server 7.0 and Microsoft SQL Server 2000 are no longer supported to the site database for the Microsoft Systems Center Configuration Manager 2007 site database.

---

Microsoft System Center Configuration Manager 2007 depends on a client installation to perform management on the clients. System Center Configuration Manager 2007 clients can be installed in one of the following manners:

- Client Push Installation
- Software Update Point Based Installation
- Group Policy Installation (most preferred)
- Manual Installation
- Logon Script Installation
- Software Distribution Installation
- Installation Using Computer Imaging

Microsoft System Center Configuration Manager 2007 clients receive agents that can be disabled or enabled as needed. Agents can be configured and pushed down during the client installation from the Microsoft System Configuration Manager 2007 Management Console. You would like to have your agents set in the management console before the client installations—otherwise you will have to wait 60 minutes to collect the data (policy default refresh point). Most agents are turned on by default. The following list is the available agents and whether or not they are enabled by default:

- Hardware Inventory Client Agent (Enabled)
- Software Inventory Client Agent (Enabled)
- Advertised Programs Client Agent (Enabled)
- Computer Client Agent (Enabled—Cannot Be Disabled)
- Desired Configuration Management Client Agent (Enabled)
- Mobile Device Client Agent (Disabled)

- Remote Tools Client Agent (Enabled)
- Network Access Protection Client Agent (Disabled)
- Software Meeting Client Agent (Enabled)
- Software Updates Client Agent (Enabled)

## EXERCISE 6.7

---

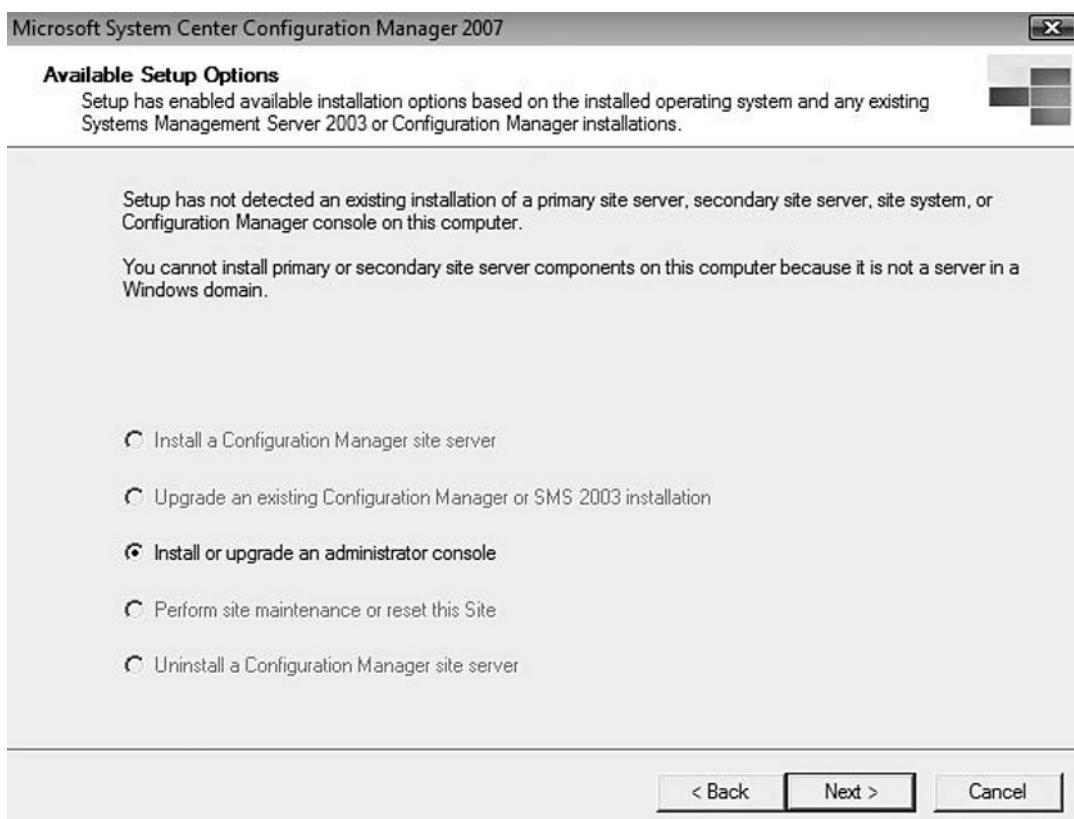
### INSTALLING THE MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER 2007 MANAGEMENT CONSOLE ON MICROSOFT WINDOWS VISTA

These following exercises assume you have Microsoft System Center Configuration Manager 2007 installed on ADSERVER01 and have a Microsoft Windows Vista client that is able to log on to the CONTOSO domain provided by ADSERVER01. As mentioned earlier—there are many prerequisites, including Microsoft SQL Server 2005, that are needed for installing Microsoft System Center Configuration Manager 2007. You can download Microsoft SQL Server 2005 as a trial download. This exercise is performed on the Microsoft Windows Vista client.

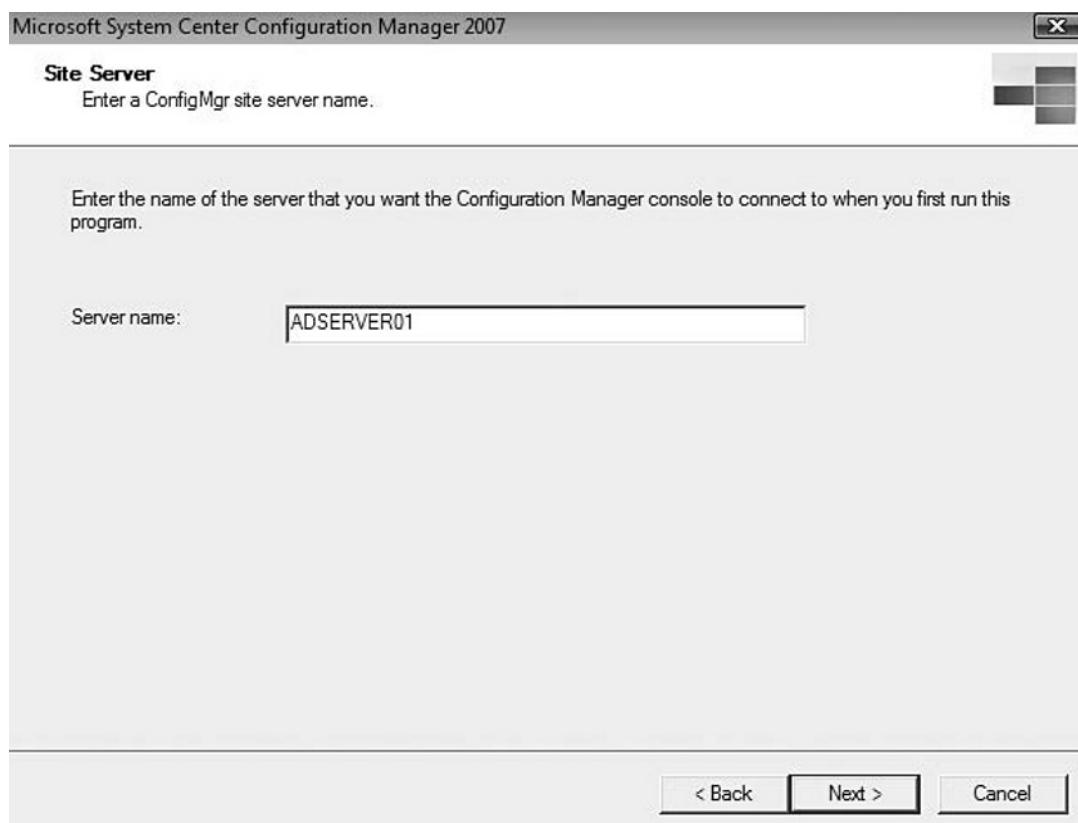
1. Insert the Microsoft System Center Configuration Manager 2007 DVD into the Microsoft Windows Vista client. The splash screen will come up (if it does not, right-click on your DVD drive and select AutoPlay)—see Figure 6.26 for Microsoft System Center Configuration Manager 2007 splash screen.

**Figure 6.26** Microsoft System Center Configuration Manager 2007 Splash Screen

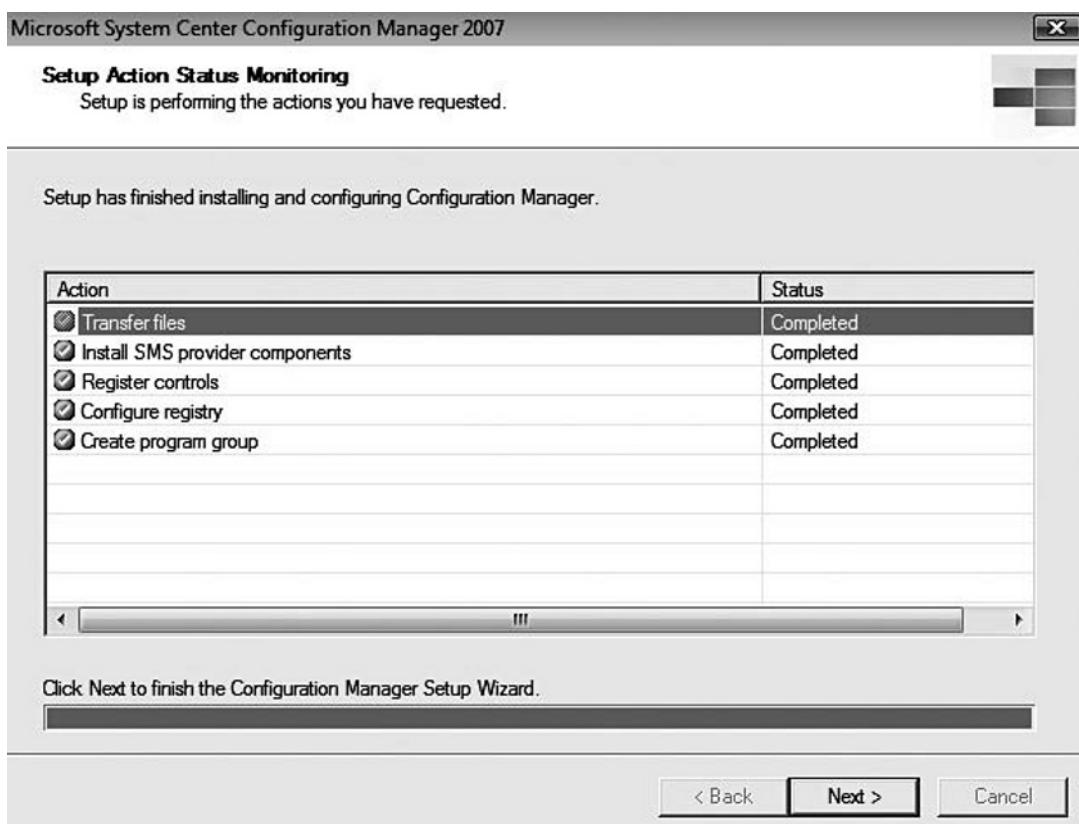
2. Under Install, click **Configuration Manager 2007**.
3. At the **Welcome to the Microsoft System Center Configuration Manager 2007 Setup Wizard**, click **Next**.
4. Verify that **Install or upgrade an administrator console** is selected in the **Available Setup Options** screen and then click **Next**—see Figure 6.27.

**Figure 6.27 Available Setup Options**

5. Select the **I accept these license terms** and click **Next**.
6. Accept the default on the **Customer Experience Improvement Program Configuration** and click **Next**.
7. Accept the default **Destination Folder** and click **Next**.
8. On the **Site Server** window—enter **ADSERVER01** for the Server name and click **Next**. See Figure 6.28.

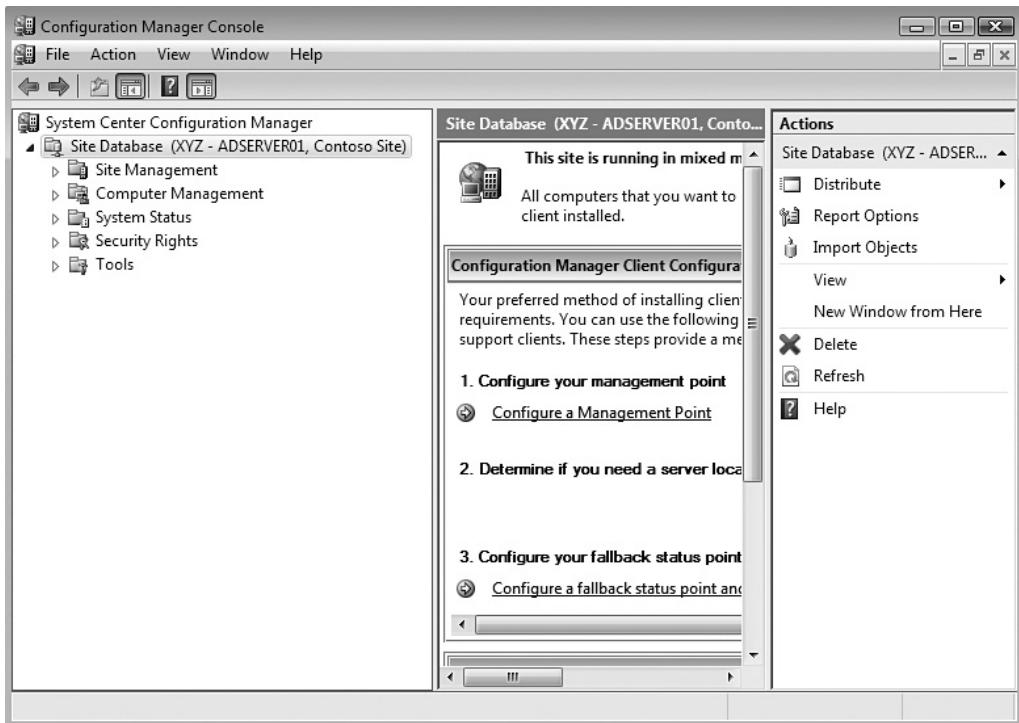
**Figure 6.28** Site Server

9. Accept the **Settings Summary** page and click **Next**.
10. The installer will perform an **Installation Prerequisites Check**. If this check is a **Success**—click **Begin Install**. If by chance the installation would have a requirement, you could double-click the message next to the requirement and it would advise you how to fix it.
11. Once the installation completes successfully (see Figure 6.29), click **Next** to continue.

**Figure 6.29** Setup Action Status Monitoring

12. Select the **Launch Configuration Manager console after closing** and click **Finish**. Figure 6.30 depicts the Microsoft System Center Configuration Manager 2007 Management Console. Click **File**, and then **Exit** to close the Microsoft System Center Configuration Manager 2007 Management Console.

**Figure 6.30 Microsoft System Center Configuration Manager 2007 Management Console**



## EXERCISE 6.8

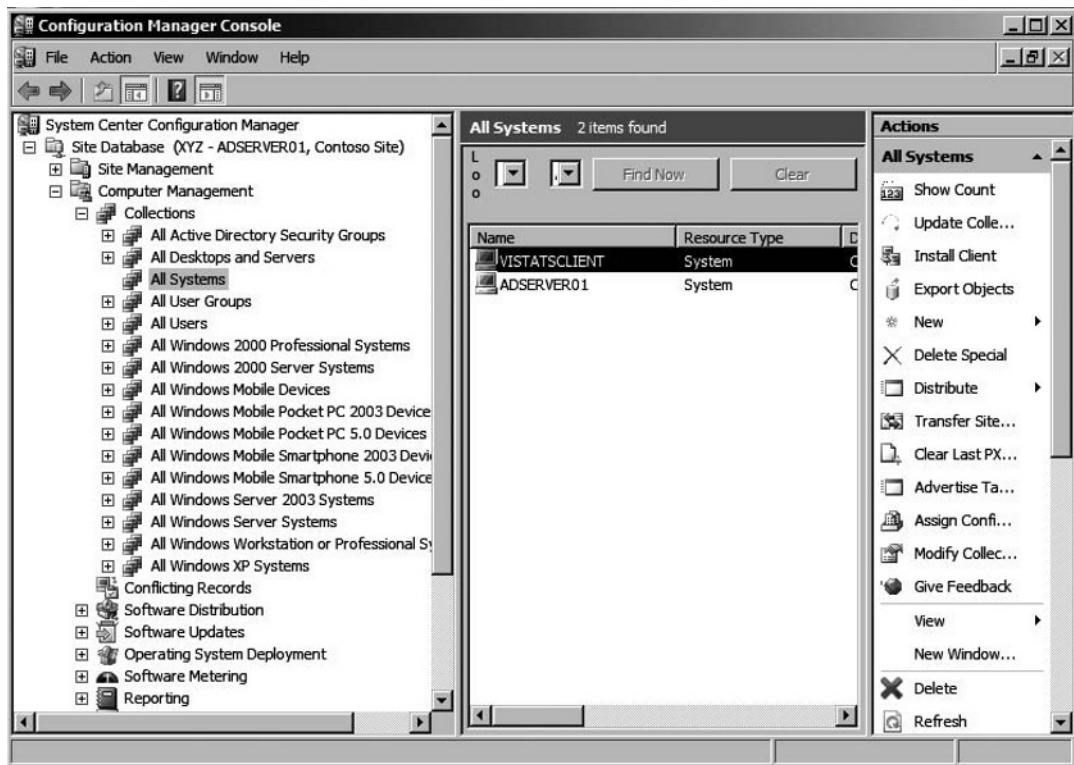
### INSTALLING THE MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER 2007 CLIENT

In this exercise, we are going to install the client software on our Microsoft Windows Vista client using the manual installation method. All of this exercise will be performed on the Microsoft Windows Vista client.

1. Logon to your Windows Vista client as Administrator on the domain CONTOSO.
2. Click **Start**, and clear **Start Search**. Type **\AD SERVER01** and press **Enter**.
3. Double-click the **SMS\_XYZ** folder. XYZ will be your 3 digit location ID you set during the Microsoft System Center Configuration Manager 2007 installation.

4. Double-click the **Client** folder.
5. Double-click the **CCMSETUP.EXE** program in this folder.
6. This will install the Microsoft System Center Configuration Manager 2007 silently. After a few minutes, go to the **ADSERVER01**.
7. Click **Start**, and then **All Programs**. Select the **Microsoft System Center** folder, and then click on **ConfigMgr Console**.
8. Expand **Computer Management** and then **Collections**. Select **All Systems** and you will see your client in the right pane. See Figure 6.31.

**Figure 6.31** Configuration Manager Console



9. Click **File**, and then **Exit** to close the Microsoft System Center Configuration Manager 2007 Management Console.

## Hardware Inventory

One of the most sought after features of Microsoft System Center Configuration Manager 2007 Management Console is the hardware inventory. The latest version of System Center Configuration Manager is capable of querying 1,500 different hardware properties. The agent that is responsible for collecting hardware data is called the Hardware Inventory Client Agent and is enabled by default. The Hardware Inventory Client Agent uses the Windows Management Instrumentation (WMI) to collect data from the client computers.

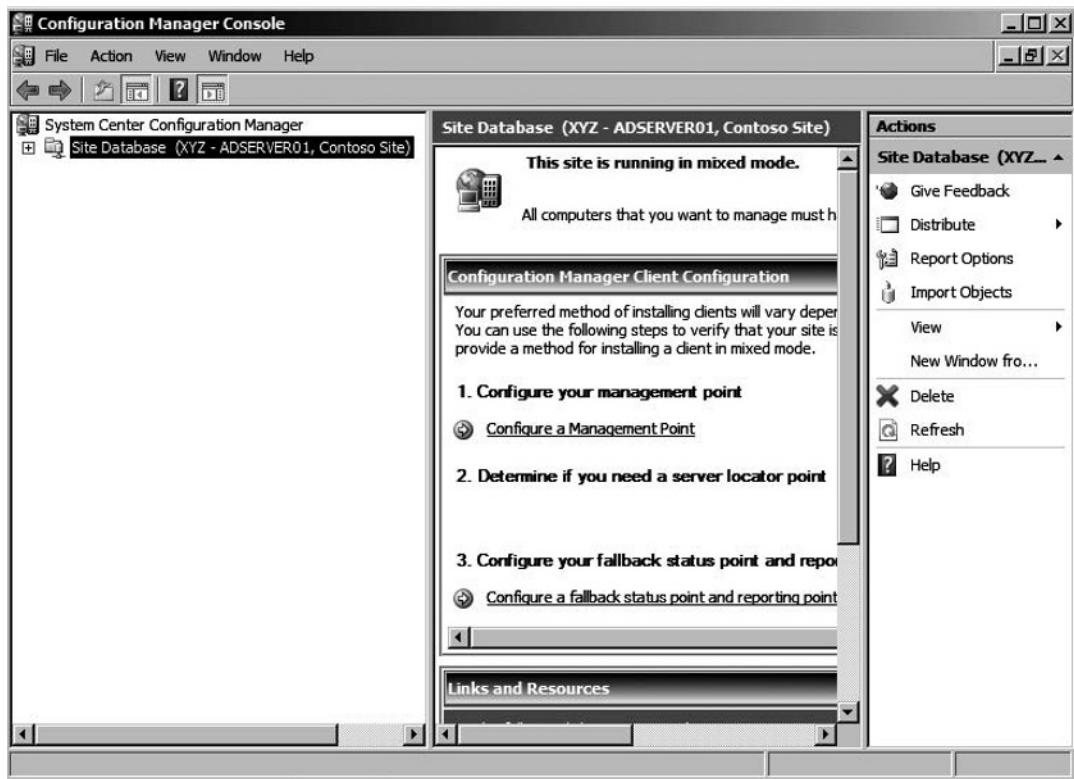
### EXERCISE 6.9

---

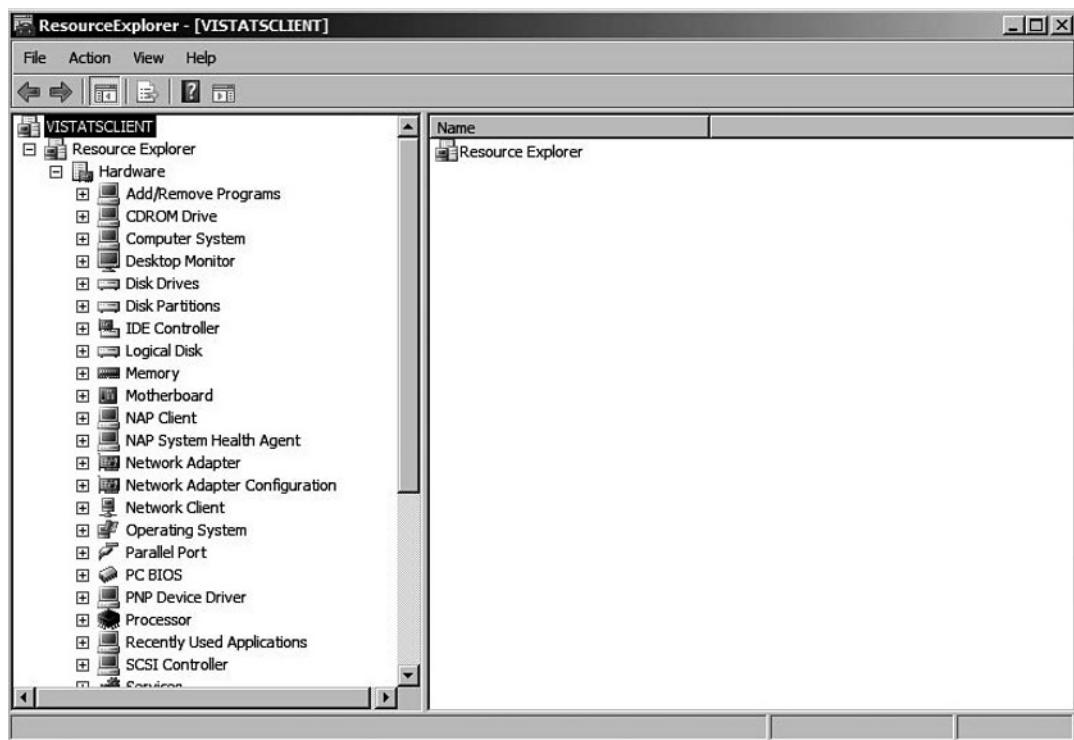
#### VIEW HARDWARE CHARACTERISTICS OF MICROSOFT WINDOWS VISTA CLIENT

In this exercise, we are going to look at some of the hardware information that is being collected on the Microsoft Windows Vista client that we installed earlier on Microsoft System Center Configuration Manager 2007. In this example, we will be using the ADSERVER01 and the Microsoft System Center Configuration Manager 2007 Management Console.

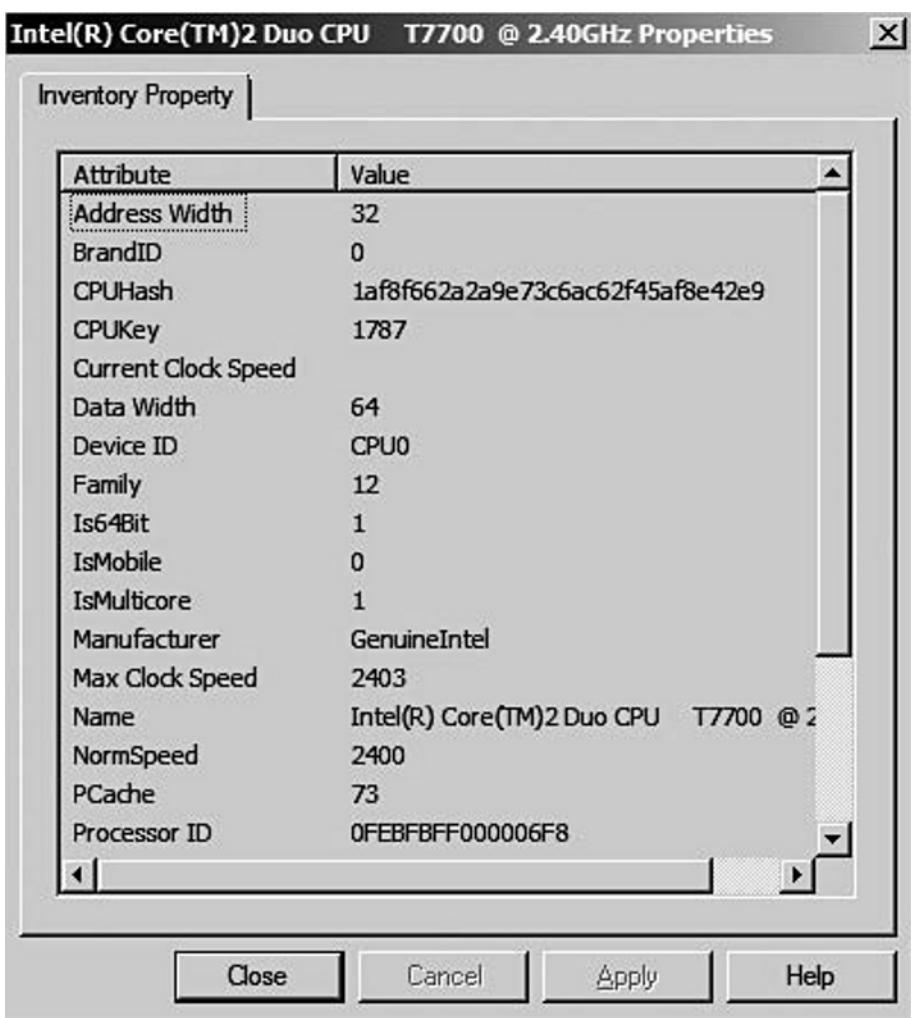
1. Click **Start**, and then **All Programs**. Select the **Microsoft System Center** folder, and then click on **ConfigMgr Console**. See Figure 6.32.

**Figure 6.32 Configuration Manager Console**

2. Expand Computer Management, and then Collections. Then select All Systems.
3. Right-click on VSTATSCLIENT (or your Windows Vista client) and select Start, and the Resource Explorer.
4. Expand Resource Explorer and then Hardware. See Figure 6.33. Notice all of the available categories available to query.

**Figure 6.33** Resource Explorer

5. Click on **Motherboard**, and in the right pane double-click the **Processor** listed. See the information listed for the processor? See Figure 6.34 as an example.

**Figure 6.34** Processor Properties

6. Click **Close** to exit the property windows. Click **File**, and then **Exit** to close the **Resource Explorer**.
7. Click **File**, and then **Exit** to close the Microsoft System Center Configuration Manager 2007 Management Console.

## Software Inventory

Just like hardware inventory, Microsoft System Center Configuration Manager 2007 is capable of software inventory. This is very important—this helps to keep

your software licenses legal which is becoming harder to do as the enterprise continues to grow. The agent responsible for software inventory is the Software Inventory Client Agent. The Software Inventory Client Agent queries the Windows Management Instrumentation (WMI) for EXE files. In particular, it searches for this information from the root/ccm/invagt/filesystemfile namespace.

The Software Inventory Client Agent is capable of collecting application information that includes the following information:

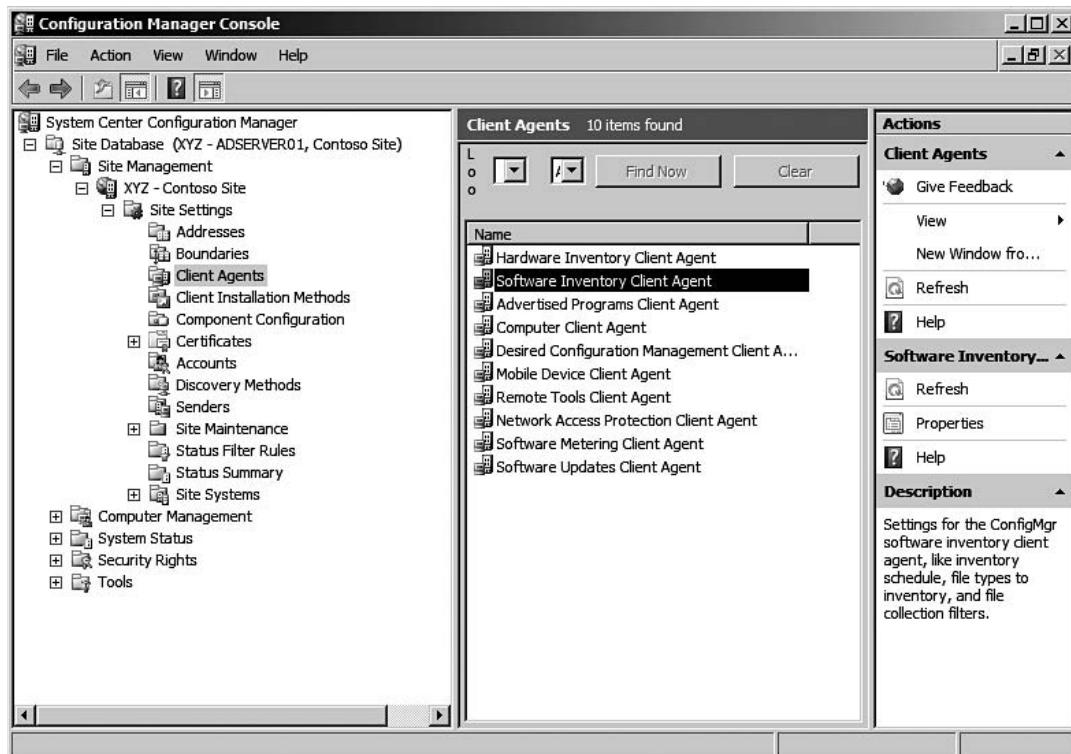
- File Name, Version, and Size
- Manufacturer Name
- Product Name, Version, and Language
- Data and Time of File Creation (at Installation)

## EXERCISE 6.10

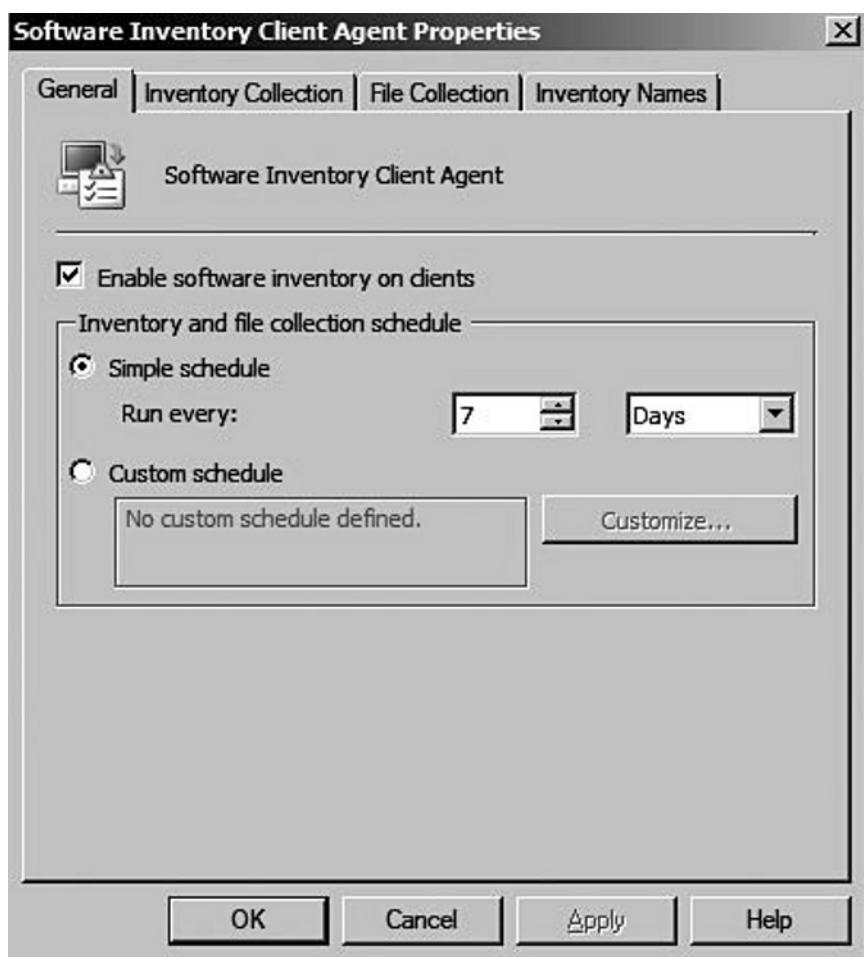
### SOFTWARE INVENTORY CLIENT AGENT

In this exercise, we are going to look at the Software Inventory Client Agent properties. The Resource Explorer for the software inventory is identical to the hardware—as a matter of fact it is in the same location. This exercise will be executed on ADSERVER01.

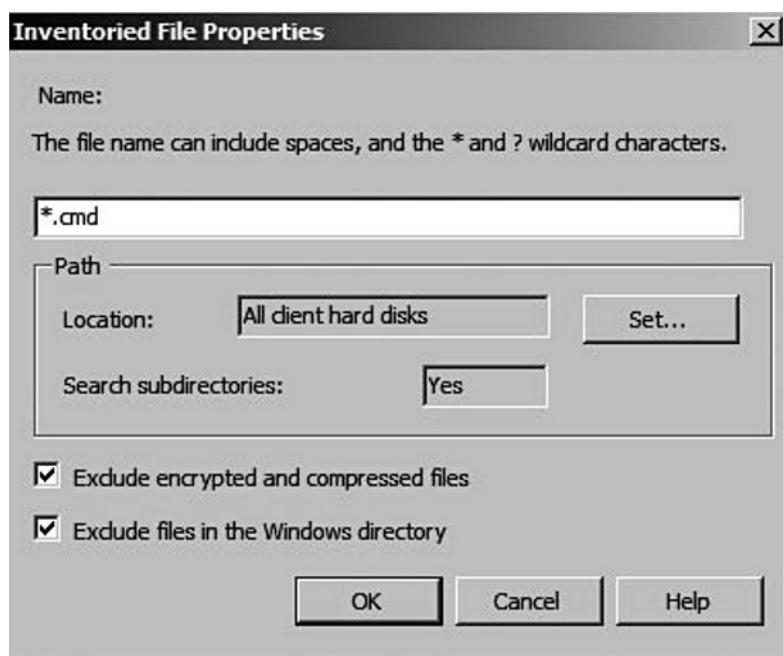
1. Click **Start**, and then **All Programs**. Select the **Microsoft System Center** folder, and then click on **ConfigMgr Console**.
2. Expand **XYZ – Contoso Site**, and then **Site Settings**.
3. Select **Software Inventory Client Agent** in the right pane.  
See Figure 6.35.

**Figure 6.35 Configuration Manager Console**

4. Right-click on the **Software Inventory Client Agent** and select **Properties**. See Figure 6.36.

**Figure 6.36 Software Inventory Client Agent Properties**

5. Change the **Run every** to **1 day**.
6. Select the **Inventory Collection** tab. Click the **add button**—this is the first button on the left.
7. The **Inventoried File Properties** windows come up. Add **\*.CMD** to the file name box. See Figure 6.37.

**Figure 6.37** Inventoried File Properties

8. Click **OK**, and then click **OK** again.
9. Click **File**, and then **Exit** to close the Microsoft System Center Configuration Manager 2007 Management Console.

---

## Application Management and Deployment

Microsoft System Center Configuration Manager 2007 has a really unique feature of being able to send applications to a workstation for installation—this is called package distribution. This is not to be confused with the OS deployment feature of Microsoft System Center Configuration Manager 2007. The agent responsible for this function is the Advertised Programs Client Agent—this is enabled by default.

When you as an administrator would like to create a package for distribution, a list of actions are required for the distribution process:

- Define your distribution points for the package.
- Create appropriate collections.

- Gather all source files, setup routines, scripts, and so on needed for the package.
- Create the Microsoft System Center Configuration Manager 2007 package.
- Define at least one program for the package.
- Distribute the package to the distribution points.
- Advertise the programs to one or more collections.

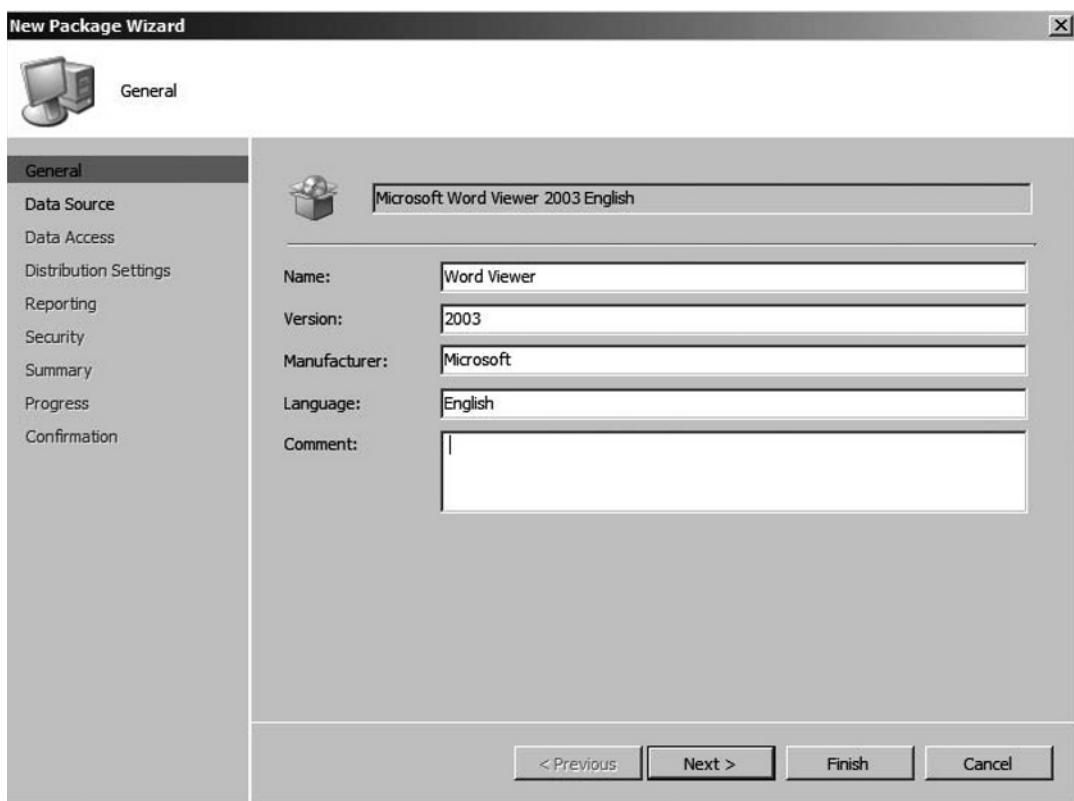
## EXERCISE 6.11

---

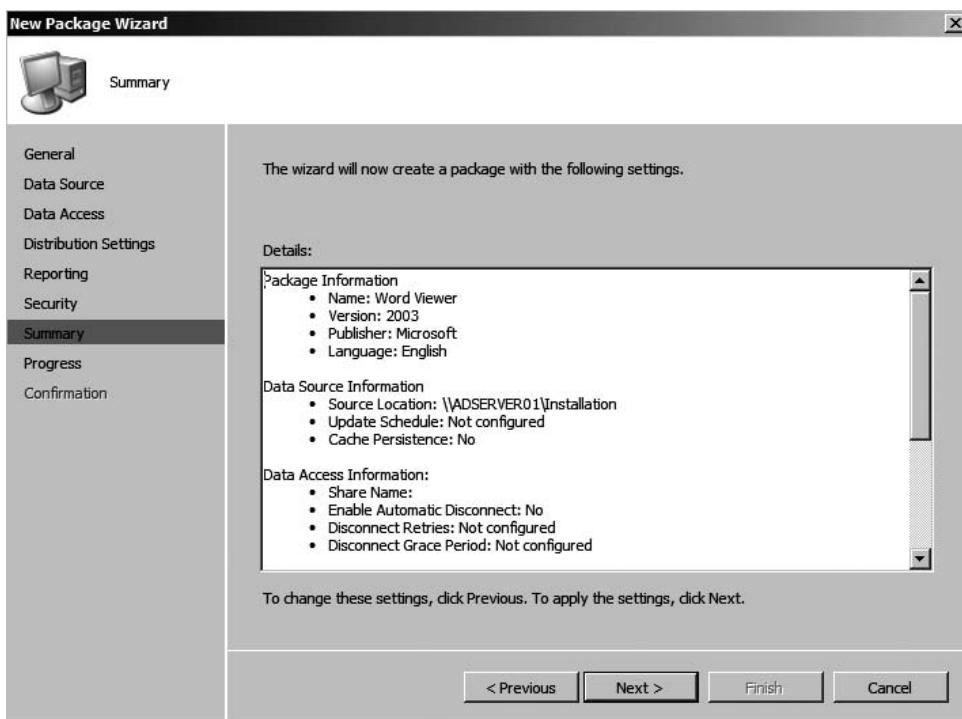
### CREATE A DISTRIBUTION PACKAGE FOR MICROSOFT WORD VIEWER

In this exercise, we are going to create a Distribution Package on ADSERVER01 for Microsoft Word Viewer and publish it for the clients on our network.

1. On the ADSERVER01, click **Start** and then **Computer**.
2. Double-click **Local Disk (C:)**.
3. Right-click and choose **New**, and then **Folder**. Name the new folder **Installation**.
4. Right-click the **Installation** folder and choose **Share**.
5. Click **Share** at the **File Sharing** windows. Click **Done** to continue.
6. Download the Microsoft Word Viewer to the Installation directory you just created. You can download the installer at <http://www.microsoft.com/downloads/details.aspx?FamilyID=3657ce88-7cfa-457a-9aec-f4f827f20cac&DisplayLang=en>.
7. Click **Start**, and then **All Programs**. Select the **Microsoft System Center** folder, and then click on **ConfigMgr Console**.
8. Expand **Computer Management**, and then **Software Distribution**. Right-click on **Packages** and choose **New**, and **Package**.
9. Then **New Package Wizard** comes up. Fill in the windows with the following information in Figure 6.38. Click **Next** to continue.

**Figure 6.38** New Package Wizard

10. Select **This package contains source files** and click the **Set** button.
11. In the **Set Source Directory**, make sure that **Network path (UNC name)** is selected. The source directory will be **\ADSERVER01\Installation**. Click **OK** to continue.
12. Click **Next** to continue.
13. Accept the default settings in the **Data Access** window and click **Next**.
14. Accept the default settings in the **Distribution Settings** window and click **Next**.
15. Accept the default settings in the **Reporting** window and click **Next**.
16. Accept the default settings in the **Security** windows and click **Next**.
17. Verify the settings in the **Summary** window—see Figure 6.39. Click **Next** to continue.

**Figure 6.39 Summary**

18. Once you get **The New Package Wizard completed successfully**, click **Close**.

---

## OS Deployment

Microsoft System Center Configuration Manager 2007 provides a means of deploying operating systems to bare systems or as upgrades. If the computer is already managed with Microsoft System Center Configuration Manager 2007, then there is no need to have an alternative media to boot the system initially. If the system has no image on it, you can choose to boot from CD sets, DVD, or USB. Network cards that support the Preboot Execution Environment (PXE) are capable of booting with no hard media. There is a definite benefit to making sure your entire network cards are PXE compatible. The image for the installation is stored on the server as a Windows Image Format (WIM) file. The WIM contains the desired Microsoft Windows operating system along with any line-of-business applications, service packs or security upgrades (basically anything installed on the base unit). The installation uses Tasks Sequences to perform the installation.

Creating an OS Deployment is beyond the scope of this examination. You just need to know the basics—you will not be expected to create installable media or perform a Task Sequence. We will not do an exercise in this section.

## Provisioning Data

The definition of a shared resource is a volume, folder, file, printer, or serial port shared over the network using the SMB protocol. In this section, we are going to look at some of the storage topics in Microsoft Windows 2008 Server. Microsoft Windows 2008 Server has built on many features from Microsoft Windows 2003 Server and has added many new features. Microsoft has added a new MMC tool called the File System Resource Manager to help you better administer file servers.

## Working with Shared Resources

One of the first updated share and files system feature is the Microsoft Windows 2008 Server Distributed File Systems (DFS). The DFS technologies offer wide area network (WAN) friendly replication as well as simplified, high availability access to geographically dispersed file systems. In Microsoft Windows 2008 Server, DFS is implemented as a role service of the File Services role. The Distributed File System role service consists of two child role services:

- DFS Namespaces
- DFS Replication

DFS is made up of four objects—below is the object with its definition:

- **Namespace Server** A server that hosts a namespace. The namespace server can be a member server or a domain controller.
- **Namespace Root** The root is the starting point of the namespace. This is a domain name-based namespace, because it begins with a domain name (for example, CONTOSO) and its metadata is stored in Active Directory. A domain namespace can be hosted on multiple name space servers.
- **Folder** Folders build the namespace hierarchy. Folders can optionally have folder targets. When users browse a folder with targets in the namespace, the client computer receives a referral that directs the client computer to one of the folder targets.
- **Folder Targets** A folder target is a Universal Naming Convention (UNC) path of a shared folder or another namespace that is associated with a folder in a namespace.

**TEST DAY TIP**

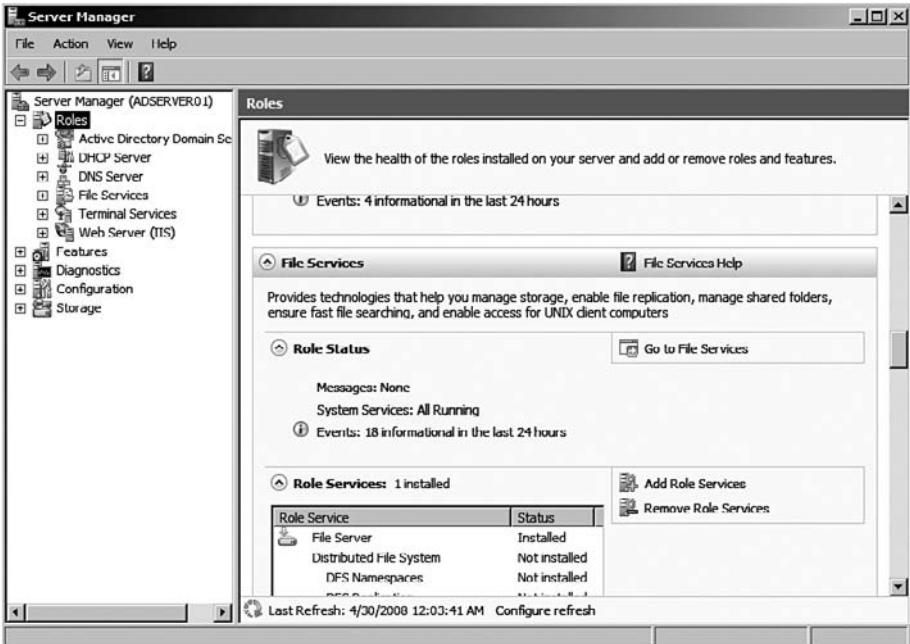
 It is very important to understand the following terms on this exam: Namespace Server, Namespace Root, Folder, and Folder Target. It is very easy to misunderstand a question because you don't know the proper definition or explanation of a term.

**EXERCISE 6.12****INSTALLING THE MICROSOFT  
WINDOWS 2008 SERVER DISTRIBUTED FILE SYSTEM**

In this exercise, we are going to install the Distributed File System on the AD SERVER01. This is a pretty straightforward exercise—just keep in mind that DFS is part of the File Server role.

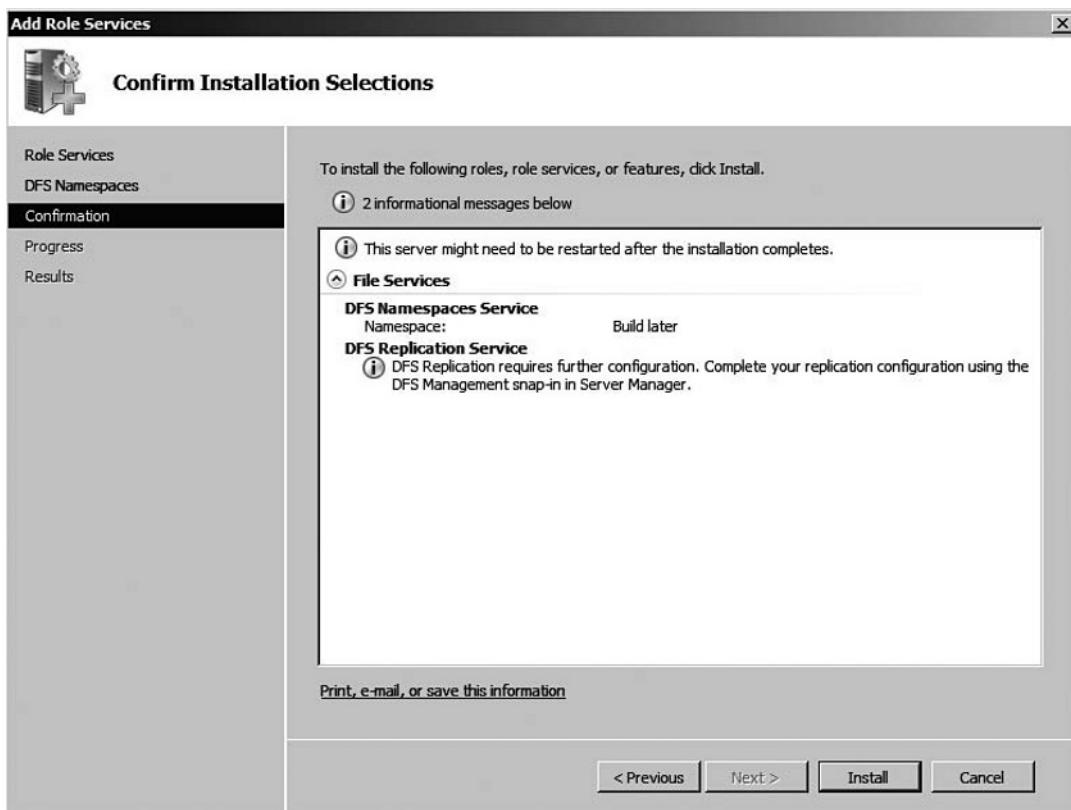
1. Click **Start**, and then **Server Manager**.
2. Click **Roles**, and then scroll the right pane down to **File Services** role. Click **Add Role Services**. See Figure 6.40.

**Figure 6.40** Server Manager



3. Select the **Distributed File System** and click **Next**.
4. In the **Create a DFS Namespace**, select **Create a namespace later using the DFS Management snap-in in Server Manager**—click **Next**.
5. In the **Confirm Installation Selection**, confirm the selections and click **Install**. See Figure 6.41.

**Figure 6.41** Confirm Installation Selections



6. Click **Close** in the **Installation Results** screen.
7. Click **File**, and then **Exit** to close the **Server Manager**.

## Offline Data Access

If you have ever had a user needing to access files when a server share was down—then you can understand the need for offline data access. Using offline files, you can access files stored in workstation folders even when the network copies are unavailable.

You can do this by choosing the network files you want to make available offline, which automatically creates a copy of the network files on the users' local computer. These copies of network files that are stored on your computer are called offline files. Windows will automatically sync your offline file for you and open them whenever the network versions are unavailable.

## EXERCISE 6.13

### WORKING WITH OFFLINE FILES

In this exercise, we are going to create a folder and share it. Then, we are going to set it up for offline file access.

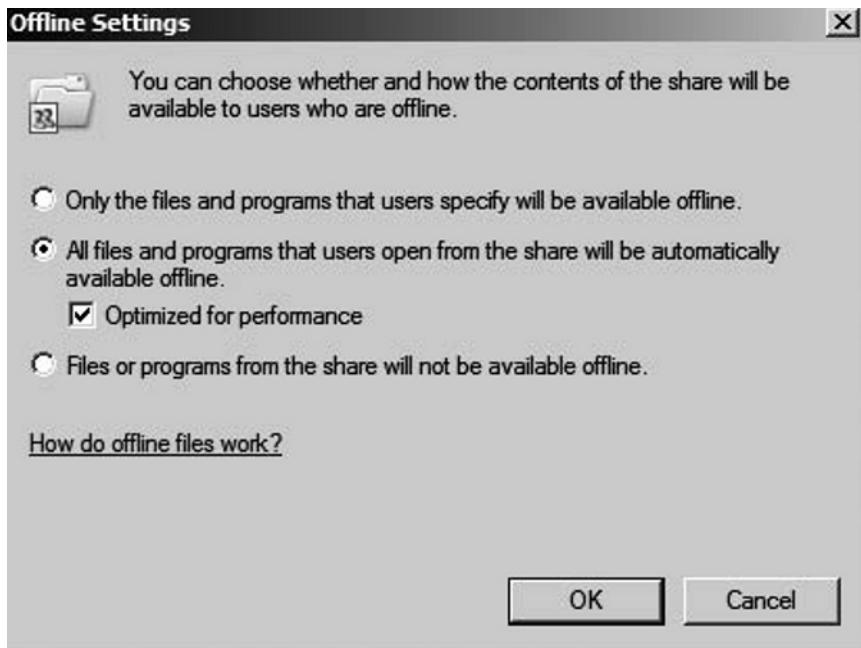
1. First, on ADSERVER01 create a folder called **Documents** in the C:\ drive.
2. Right-click the **Documents** folder and click **Properties**.
3. Under the folder properties, select the **Sharing** tab. See Figure 6.42.

**Figure 6.42** Document Properties



4. Click Advanced Sharing.
5. Select Share this folder, and then click Caching.
6. Select All files and programs that users open from the share will be automatically available offline. See Figure 6.43.

**Figure 6.43** Offline Settings



7. Click OK twice.
  8. Click Close to close the folder properties.
  9. This folder is now ready for offline file use with a Windows client.
-

## Summary of Exam Objectives

Microsoft has really stepped up their offerings in the terminal server market. The Microsoft Licensing has not changed much—you will need to contact the Microsoft License Clearinghouse to activate the terminal licenses. You do have a 120 day grace period to activate your license.

By default, Terminal Services uses port 3389 and usually is not permitted through firewalls due to security concerns. Terminal Services Gateway Server allows clients to connect from the Internet to the workplace over a secure connection. The connection is made over a HTTPS connection with RDP encapsulated. Terminal Services Gateway Server relies on the following roles and services: Remote Procedure Call (RPC) over HTTP Proxy, Internet Information Services (IIS) 7.0, and Network Policy and Access Services.

Terminal Services Session Broker (TS Session Broker) allows you to enable a user to reconnect to an existing disconnected session in a load-balanced terminal server farm, and probably more important, the TS Session Broker enables you as an administrator to distribute the session load between servers in a load-balanced server farm. The servers participating in this farm must be Microsoft Windows 2008 Servers and supported clients must be using the Remote Desktop Connection (RDC) version 5.3 or later.

Microsoft Terminal Services RemoteApp allows an administrator to publish applications to a user in a window that looks as if the application is running locally on the clients' computer. A user can minimize, maximize, and resize the program window—you can also start numerous RemoteApps on a client. TS RemoteApp is compatible with the following operating systems: Microsoft Windows Vista, Microsoft Windows 2008 Server, Microsoft Windows XP Service Pack 2, and Microsoft Windows 2003 Service Pack 1.

Resource allocation can be handled through the Microsoft Windows System Resource Manager. Microsoft Windows System Resource Manager comes with four built in Resource Management Policies, these include: Equal\_Per\_Process, Equal\_Per\_User, Equal\_Per\_Session, and Equal\_Per\_IISAppPool.

Microsoft Virtualization sometimes gets confused with Microsoft Terminal Services—they can actually work together in some cases. Microsoft Virtualization can be managed by Microsoft System Center. Microsoft has four product offerings: Microsoft Terminal Services—Presentation Virtualization, Microsoft Virtual Server 2005 R2—Server Virtualization, Microsoft Virtual PC 2007—Desktop Virtualization and Microsoft SoftGrid— and Application Virtualization.

Microsoft System Configuration Manager 2007 provides monitoring along with configuration for software and hardware in a Microsoft platform environment. Microsoft System Center Configuration Manager 2007 clients receive agents that can be disabled or enabled as needed. Agents can be configured and pushed down during the client installation from the Microsoft System Configuration Manager 2007 Management Console. Most agents are turned on by default.

The latest version of System Center Configuration Manager is capable of querying 1,500 different hardware properties. The agent that is responsible for collecting hardware data is called the Hardware Inventory Client Agent and is enabled by default. The Hardware and Software Inventory Client Agent uses the Windows Management Instrumentation (WMI) to collect data from the client computers.

Microsoft System Center Configuration Manager 2007 has a really unique feature of being able to send applications to a workstation for installation—this is called package distribution. This is not to be confused with the OS deployment feature of Microsoft System Center Configuration Manager 2007. The agent responsible for this function is the Advertised Programs Client Agent—this is enabled by default.

Microsoft System Center Configuration Manager 2007 provides a means of deploying operating systems to bare systems or as upgrades. If the computer is already managed with Microsoft System Center Configuration Manager 2007, then there is no need to have an alternative media to boot the system initially. If the system has no image on it, you can choose to boot from CD sets, DVD, or USB. Network cards that support the Preboot Execution Environment (PXE) are capable of booting with no hard media. The image for the installation is stored on the server as a Windows Image Format (WIM) file.

The DFS technologies offer wide area network (WAN) friendly replication as well as simplified, high availability access to geographically dispersed file systems. The Distributed File System role service consists of two child role services—DFS Namespaces and DFS Replication. Offline files can be stored in local workstation folders even when the network copies are unavailable.

## Exam Objectives Fast Track

### Understanding Virtualization in Windows Server 2008

- Microsoft Terminal Server—Presentation Virtualization
- Microsoft Virtual Server 2005 R2—Server Virtualization
- Microsoft Virtual PC 2007—Desktop Virtualization
- Microsoft SoftGrid—Application Virtualization
- Microsoft SoftGrid was purchased from Softricity.

### Provisioning Applications

- Terminal Services Licensing manages the terminal services client access licenses.
- Terminal Services Gateway Server allows RDP connections to securely connect over the Internet via the HTTPS over SSL to terminal servers or internal network resources.
- Terminal Session Broker allows for load-balancing server farms and reconnects disconnected sessions.
- Microsoft Terminal Services RemoteApp allows an administrator to publish applications to a user in a window that looks as if the application is running locally on the clients' computer.
- Microsoft Windows System Resource Manager is used to allocate server resources according to priority.

### System Center Configuration Manager

- Microsoft System Center Configuration Manager 2007 allows you to perform and automate many administrative tasks.
- Microsoft SQL Server 2005 Service Pack 2 is now required to host the site database for Microsoft System Center Configuration Manager 2007.
- Microsoft System Center Configuration Manager 2007 clients receive agents that can be disabled or enabled as needed—these agents collect specific data or perform specific tasks.
- The Hardware Inventory Client Agent uses the Windows Management Instrumentation (WMI) to collect data from the client computers.

## Provisioning Data

- The definition of a shared resource is a volume, folder, file, printer, or serial port shared over the network using the SMB protocol.
- The DFS technologies offer wide area network (WAN) friendly replication as well as simplified, high available access to geographically dispersed file systems.
- The Distributed File System role service consists of two child role services—DFS Namespaces and DFS Replication
- Offline files can be stored in local workstation folders even when the network copies are unavailable.

# Exam Objectives

## Frequently Asked Questions

**Q:** This chapter has a lot of new acronyms that I have never heard before. Will the exam use acronyms and what is the best way to learn them?

**A:** The exam will definitely use acronyms to try and throw you off on a question. The best way to learn acronyms is to use index cards to make flash cards.

**Q:** My employer has not installed or migrated to Microsoft Windows Server 2008 or Microsoft System Center Configuration Manager 2007 yet. Should I get hands on experience before sitting this exam?

**A:** Yes! The best advice for any Microsoft exam is to actually sit down and work with the product. Go out and download the free copy of Microsoft Virtual PC 2007 and register for a 180 day trial of Windows Server 2008 Enterprise Edition and Microsoft System Center Configuration Manager 2007. With Microsoft Virtual PC 2007, you can use multiple virtual machines to build virtual networks. This way you can setup just about any scenario in a test environment.

**Q:** In this chapter, you mentioned that Microsoft Windows System Resource Manager (WSRM) is only available with Microsoft Windows Server 2008 Enterprise Edition. Will the exam cover Microsoft Windows Server 2008 Enterprise Edition?

**A:** Microsoft Windows Server 2008 Enterprise Edition is fair game on this exam. It is important to understand what WSRM does and how to manipulate settings and create Process Matching Criteria and policies.

**Q:** What is the information in this chapter that causes students the most problems on the exam?

**A:** I find that most students have problems understanding Terminal Service technologies; especially if they have never been in an environment that uses Terminal Services. If students have never used Terminal Services—they usually get it mixed up with RDP connections to a workstation. It is very important to understand Terminal Server, TS Licensing, TS Session Broker, TS Gateway, and TS Web Access.

**Q:** Will there be scenario based questions on the exam concerning Terminal Services?

**A:** Yes! It is very important to get your hands on some equipment you can use for training—see the question above and response concerning Microsoft Virtual PC 2007.

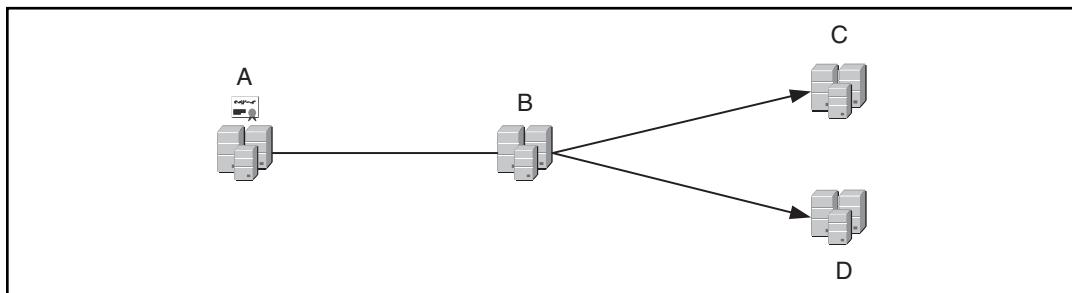
**Q:** I don't quite understand a topic in this chapter—where is the best place to go for additional information?

**A:** The best place to gather more information is right to the source—Microsoft TechNet. You can go to the site at: <http://technet.microsoft.com>.

## Self Test

1. What are the valid methods to contact Microsoft Licensing Clearinghouse to register and activate terminal server licenses?
  - A. Automatic Connection
  - B. E-mail
  - C. Web Browser
  - D. Telephone
2. When planning a terminal server infrastructure, licensing choice, and design, Microsoft provides a couple of options concerning licensing types for terminal services. What are the licensing types available in Microsoft Windows 2008 Server?
  - A. Per-Device Client Access License
  - B. Per-Server Client Access License
  - C. Per-User Client Access License
  - D. Per-Processor Access License
3. In the following Visio drawing, Figure 6.44, which letter depicts the Windows 2008 Terminal Server License Server?
  - A. A
  - B. B
  - C. C
  - D. D

**Figure 6.44** Terminal Server License Diagram



4. You boss has asked you to install Terminal Services on a Microsoft Windows 2008 Server. What would be the first step in this process?
  - A. Add the Terminal Server Role
  - B. Add the Terminal Server Feature
  - C. Add/Remove Programs
  - D. Upgrade Microsoft Windows 2008 Server to Enterprise Edition
5. Microsoft Terminal Services Gateway Server allows us to connect to a Terminal Server securely from over the Internet with no other VPN technology. What are the protocols that are involved in this process?
  - A. ICA
  - B. RDP
  - C. HTTPS
  - D. HTTP
6. Microsoft Terminal Services Gateway Server is dependent on other server roles and features that must be installed for Terminal Services Gateway Server to function properly. What are these other roles and/or features?
  - A. Remote Procedure Call (RDP) over HTTP Proxy
  - B. Application Server
  - C. Internet Information Services (IIS) 7.0
  - D. Network Policy and Access Services
7. When a client connects to a Terminal Server internally on a LAN with no encryption, what TCP port number is being used to establish this connection?
  - A. 443
  - B. 80
  - C. 3389
  - D. 1494
8. When you install Terminal Services Licensing, the server will issue temporary licenses during a “grace period.” How long do you have before this “grace period” expires?
  - A. 90 Days
  - B. 6 Months

- C. 120 Days
  - D. 180 Days
9. In Microsoft Windows 2008 Server, Microsoft includes a Terminal Service feature called the Microsoft Terminal Services Session Broker (TS Session Broker). What are the two main functions of the TS Session Broker?
- A. Enable a user to reconnect to an existing session.
  - B. Enable a user to connect over the Internet in a secured manner.
  - C. Enable session load-balancing.
  - D. Enable a user to connect to a Web site to start RDP connection.
10. You are an administrator of a midsized company. You would like to implement TS Session Broker service with two servers. One server is running Microsoft Windows 2008 Server Standard Edition and the other server is running Microsoft Windows 2003 Server Enterprise Edition. The clients are using an older copy of the Remote Desktop Connection (RDC) software. You have worked on this installation for three days and still cannot get it to work. What is likely the problem or problems?
- A. You need to upgrade the Microsoft Windows 2008 Server Standard Edition to Enterprise Edition.
  - B. The Remote Desktop Connection (RDC) software needs updated.
  - C. Microsoft Windows 2003 Server needs to be upgraded to Microsoft Windows 2008 Server.
  - D. The Microsoft Windows 2003 Server needs to have Service Pack 2 installed.

Correct Answers & Explanation: **B, C.** For TS Session Broker service to work, you must be using

## Self Test Quick Answer Key

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

This page intentionally left blank

# Chapter 7

## MCITP Exam 646

### 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*.

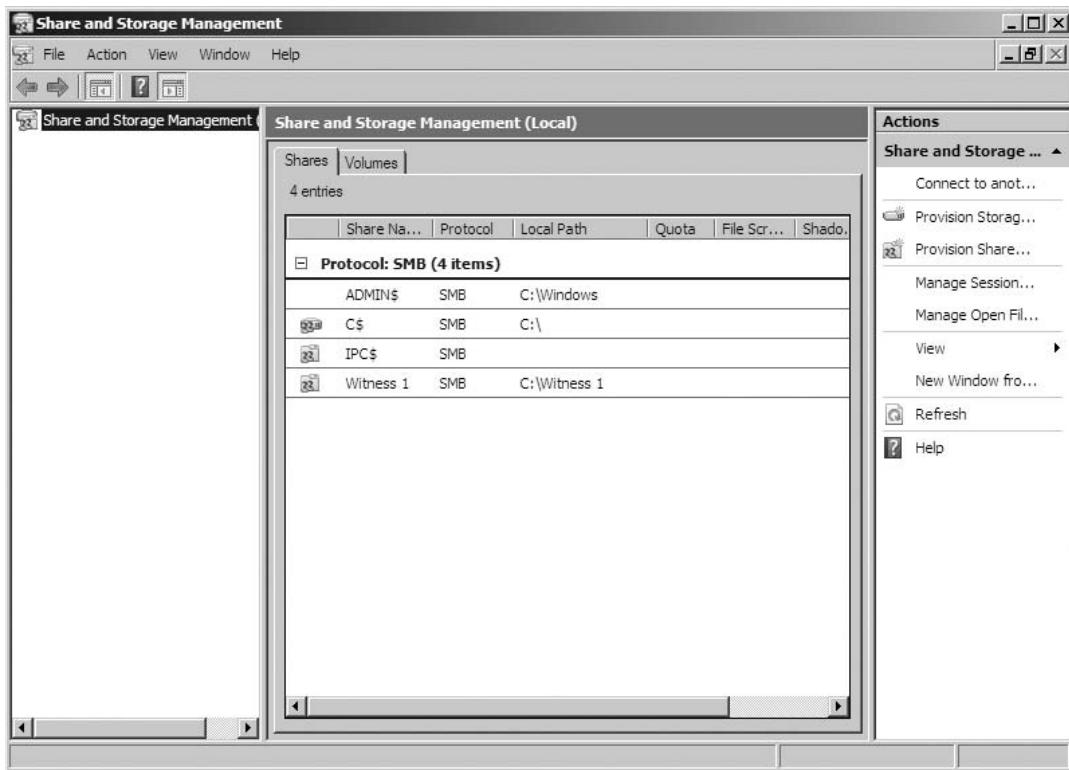
Once installed MPIO can be launched from either of 2 locations: the Control Panel or Administrative Tools. Some storage vendors have their own Device Specific Modules designed to work with W2K8. To install them, open the **MPIO Control Panel Configuration Utility | DSM** tab.

## 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.

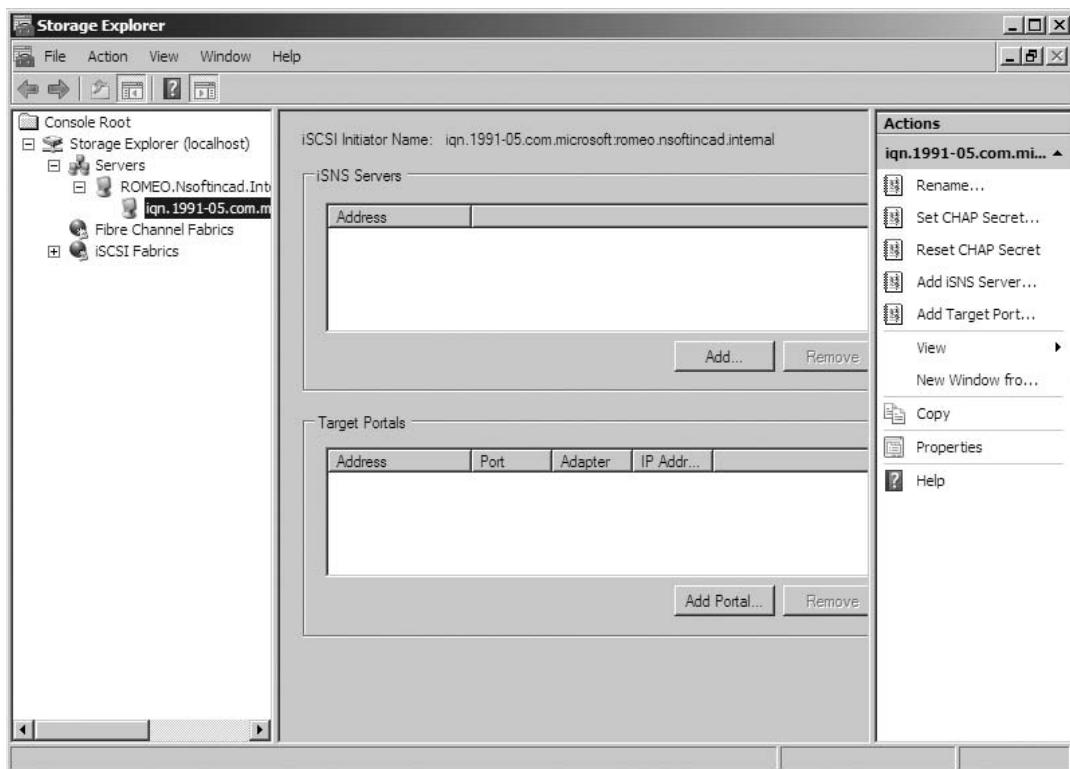
## Share and Storage Management Console

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 7.1). 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 7.1** Windows Share and Storage Management Console

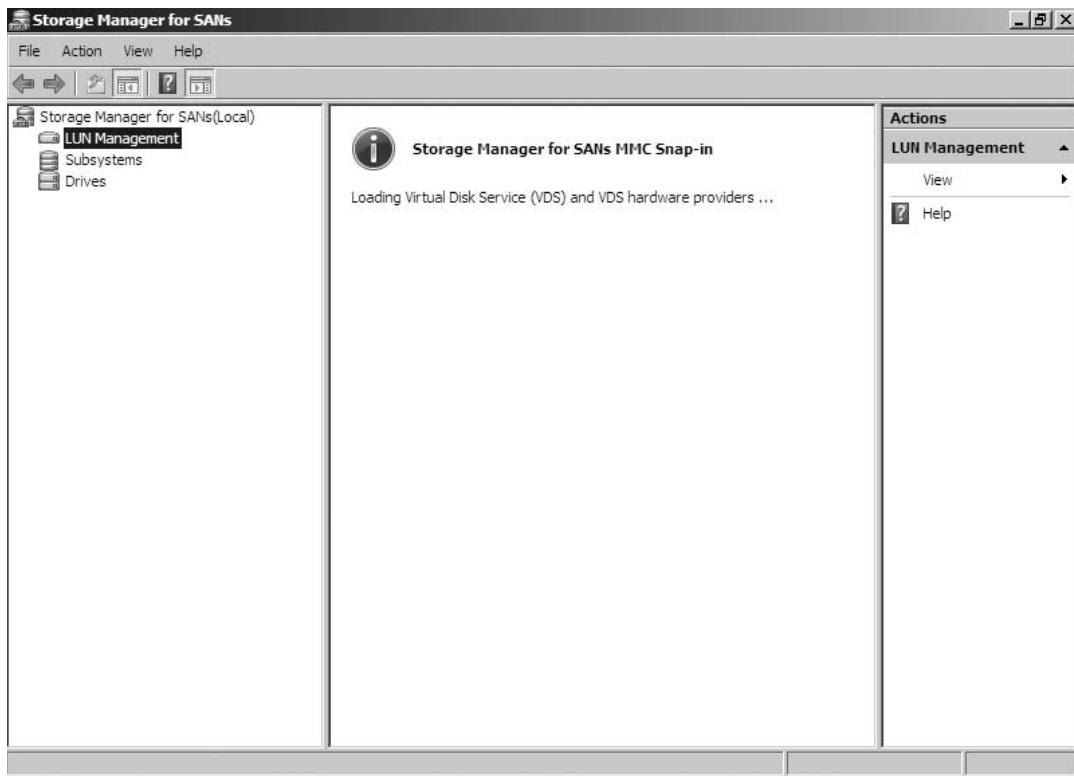
## Storage Explorer

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 7.2).

**Figure 7.2** 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 7.3. 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 7.3** 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 5 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

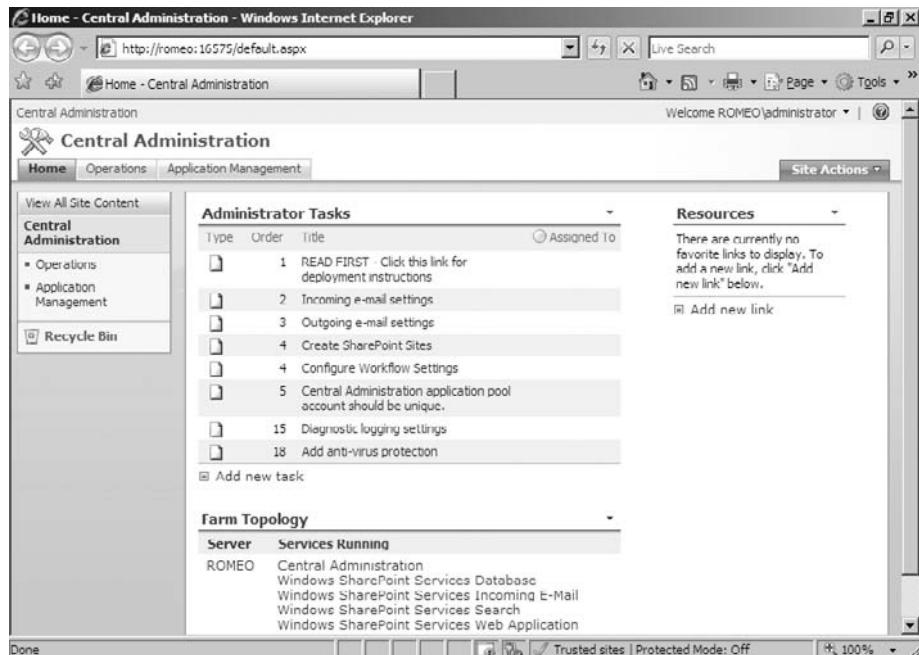
A very common scenario that I have seen develop within larger organizations is the rush for each individual department to develop and deploy their own individual Sharepoint solutions, with little to no planning or thought applied to the overall Sharepoint requirements of the organization as a whole. 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 7.4 is an example of the Windows SharePoint Services 3.0 SP1 central administration Web site.

**Figure 7.4** 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**.

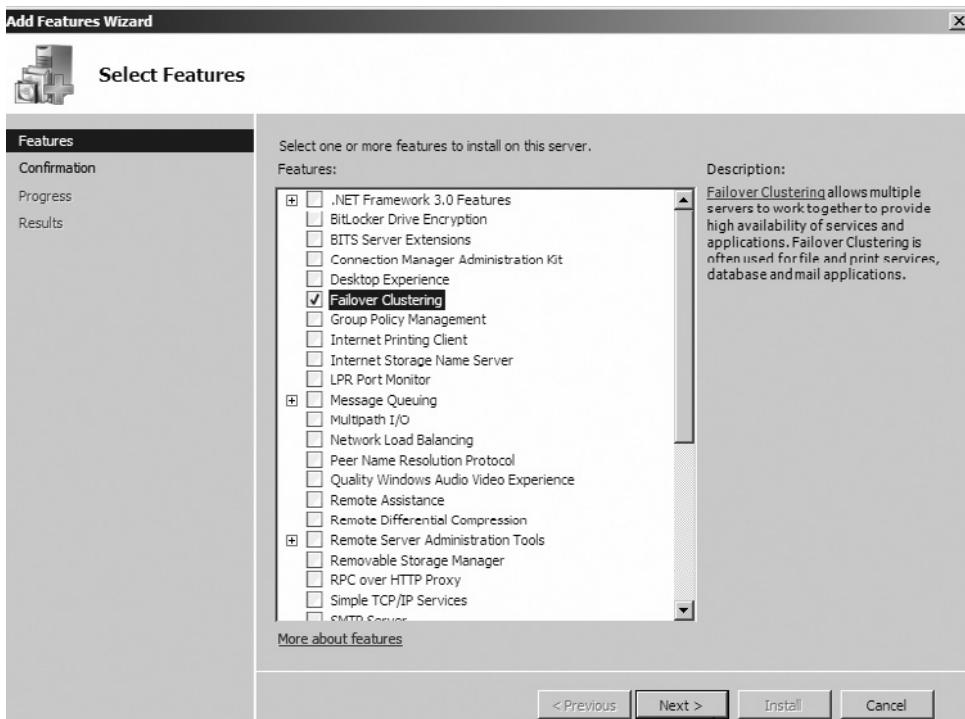
## EXERCISE 7.1

### 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.

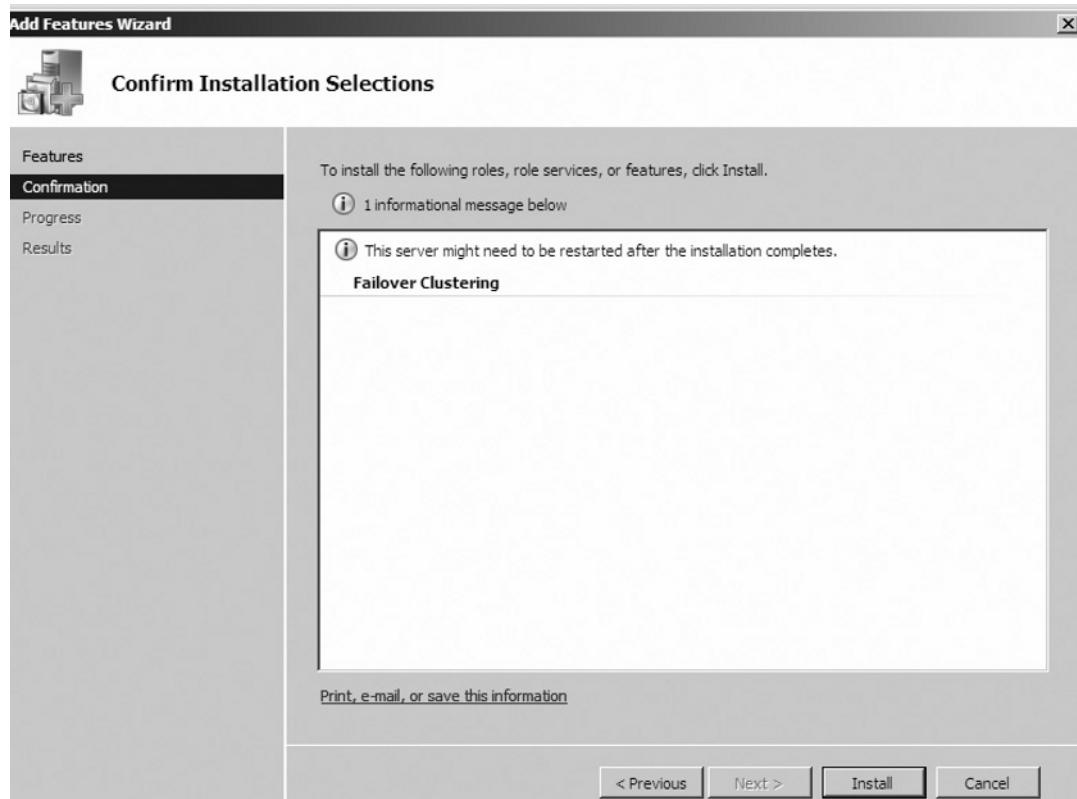
1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Features | Add Features**.
3. Select **Failover Clustering Feature** and then click **Next** to proceed (see Figure 7.5).

**Figure 7.5** Add Features Wizard “Select Features” Screen

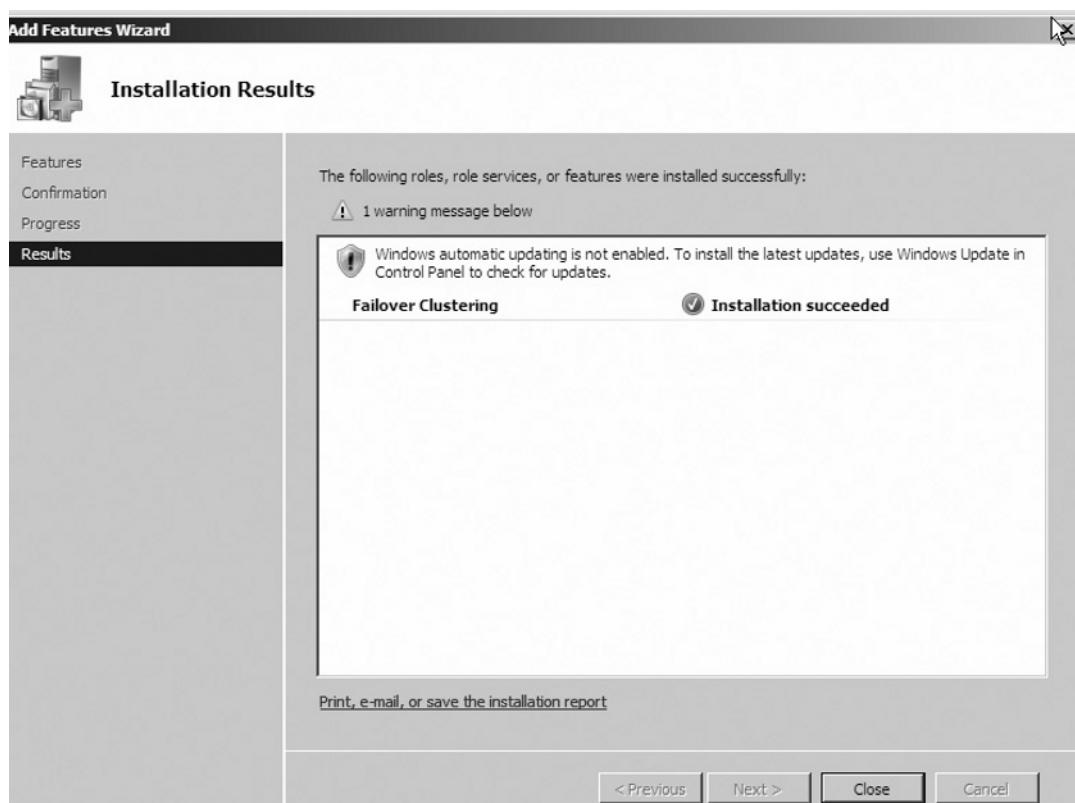


4. When the **Confirm Installation Selections** page appears, click **Install** to proceed (see Figure 7.6).

**Figure 7.6** Add Features Wizard “Confirm Installation Selections” Screen

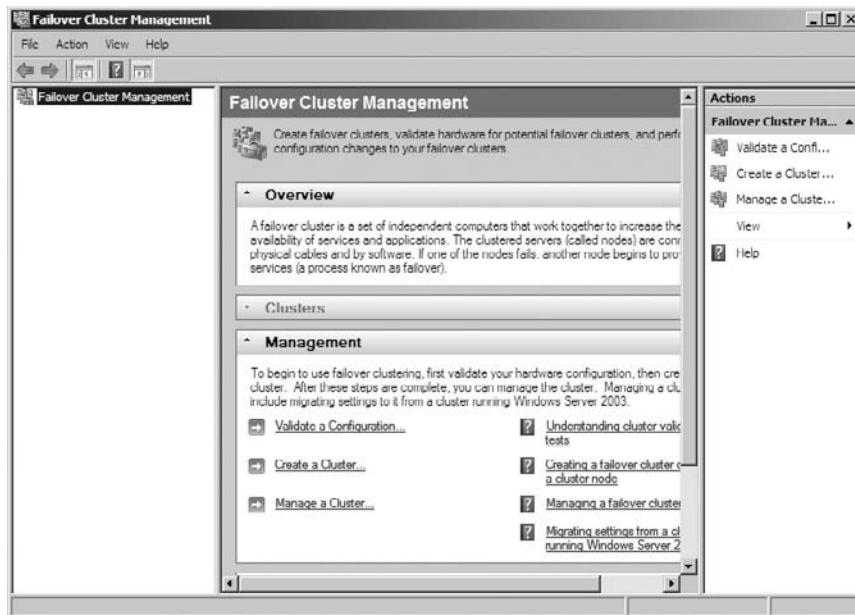


5. Once the installation is finished select, click **Close** to finish the wizard, as seen in Figure 7.7.

**Figure 7.7** Add Features Wizard “Installation Results” Screen

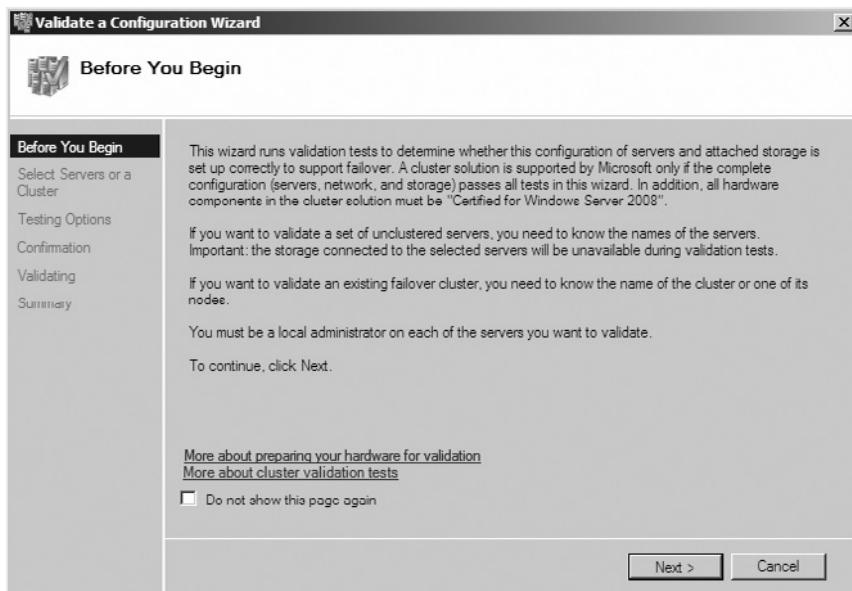
6. Select **Start | Administrative Tools | Failover Cluster Manager**.
7. In the Actions Pane in the upper right, select **Validate a Configuration** (see Figure 7.8).

**Figure 7.8 Failover Cluster Management Console—Prior to New Cluster Creation**



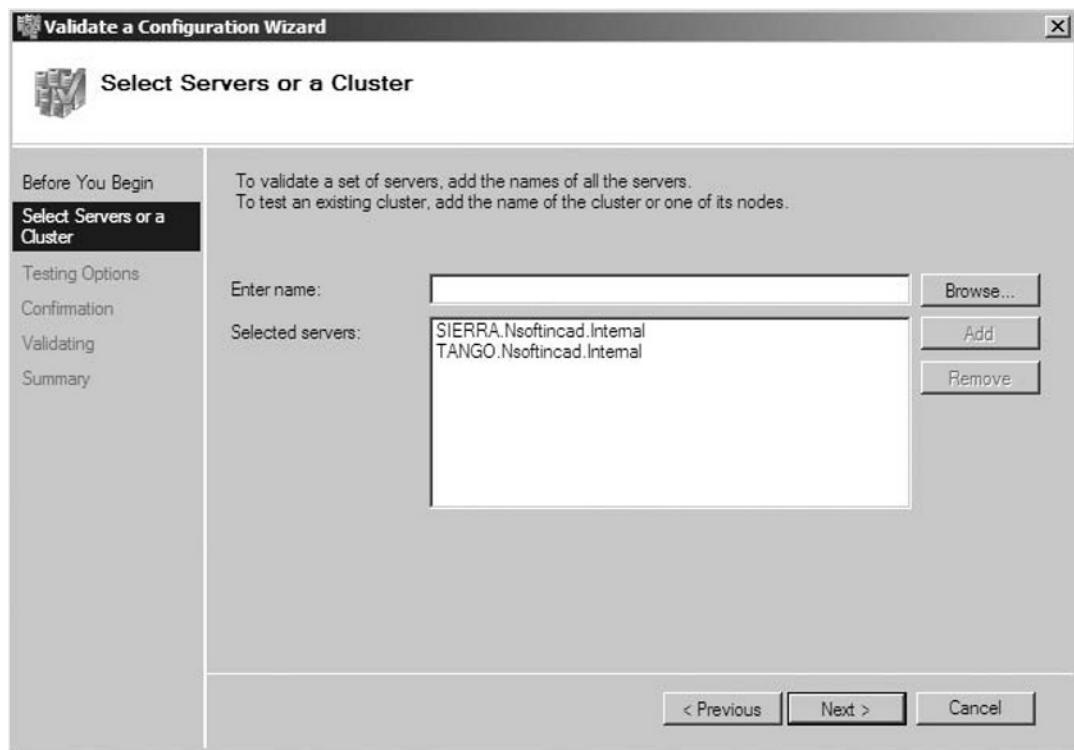
8. Read the information provided on this page, and then select **Next** to continue (see Figure 7.9).

**Figure 7.9 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 7.10).

**Figure 7.10** 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**

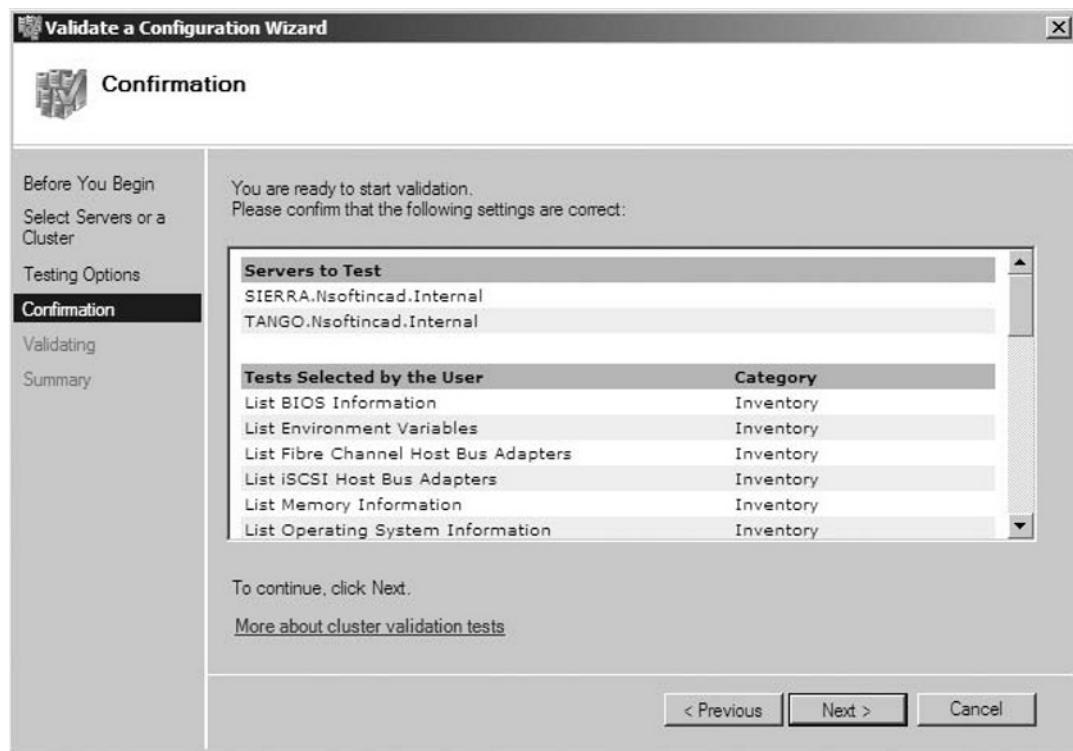
If Windows Firewall Protection is configured to block Remote Procedure Calls on the target node servers this will also cause them to report as being *Unreachable*.

10. Select the **Run all Tests (recommended)** option and then click **Next** to proceed (see Figure 7.11).

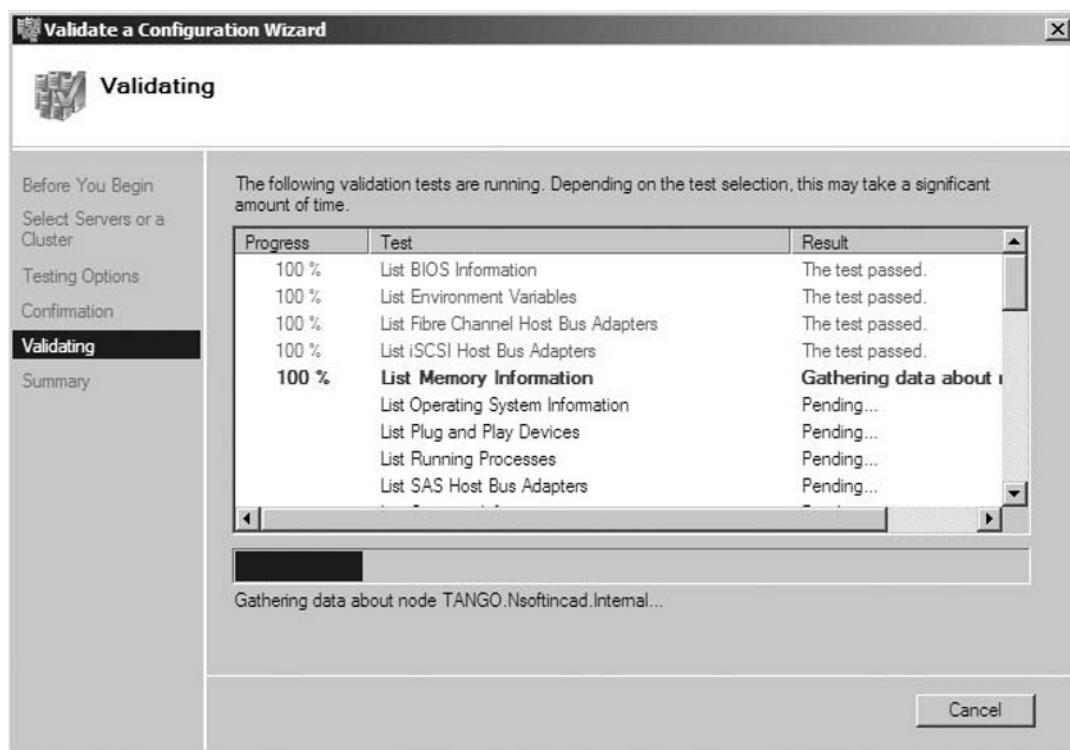
**Figure 7.11** Validate a Configuration Wizard—“Testing Options” Page



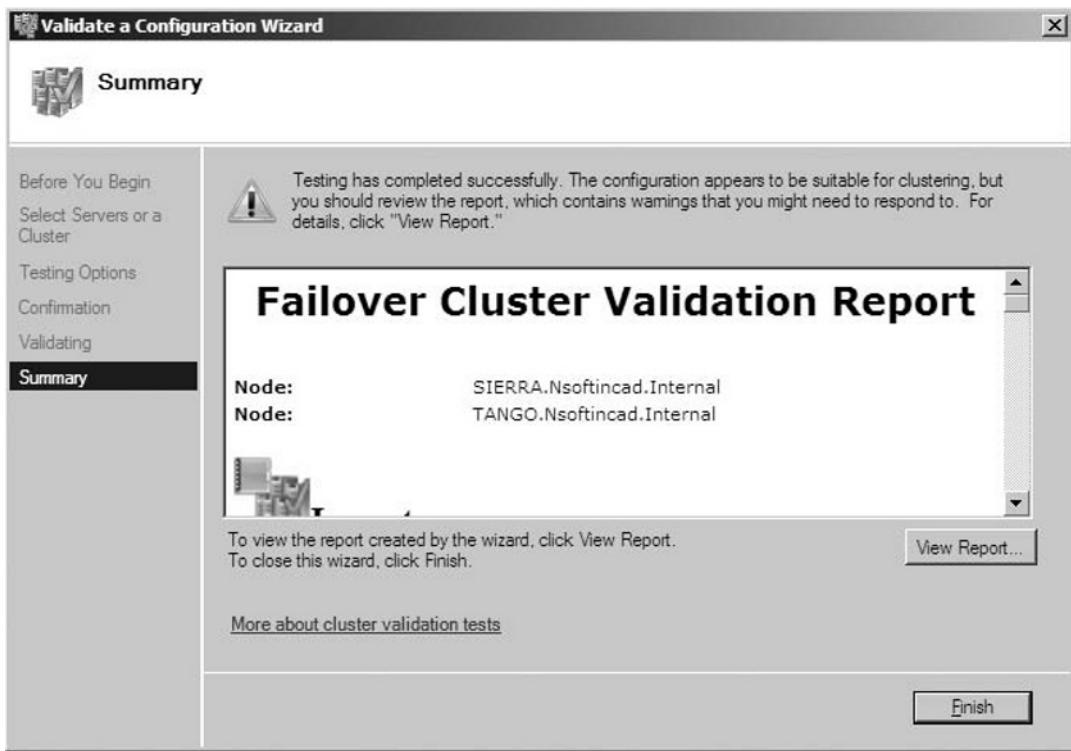
11. After confirming the selected options (see Figure 7.12), click **Next** to proceed.

**Figure 7.12** Validate a Configuration Wizard—“Confirmation” Page

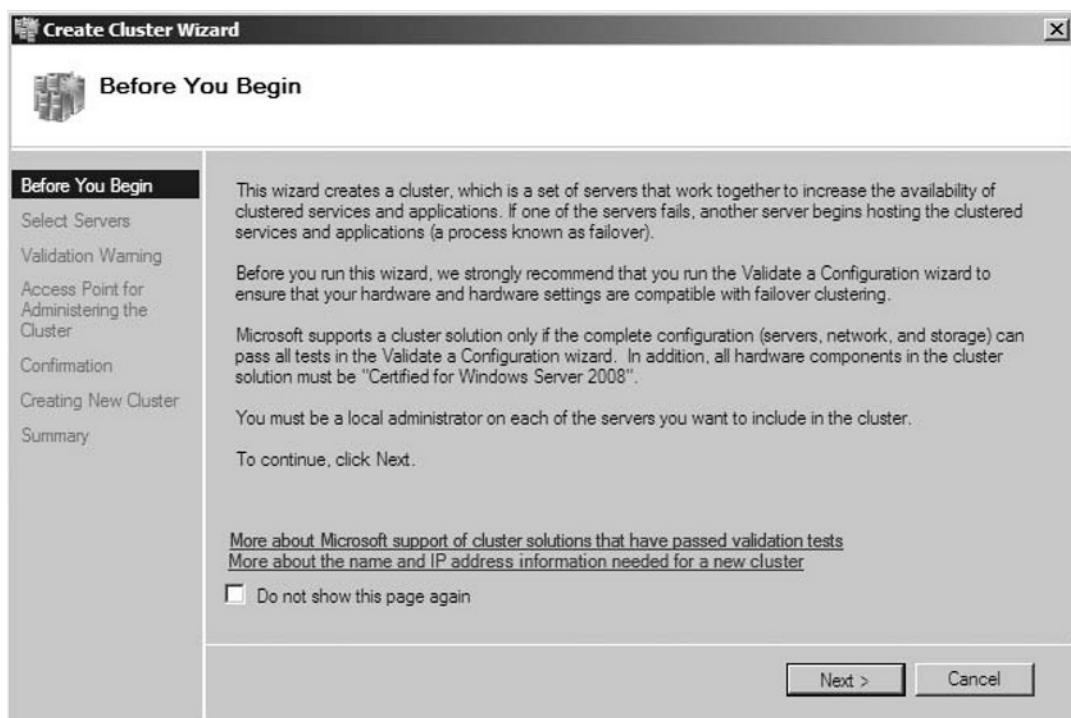
12. It will take a few minutes for the Validation process to run, as shown in Figure 7.13.

**Figure 7.13** Validate a Configuration Wizard—“Validating” Page

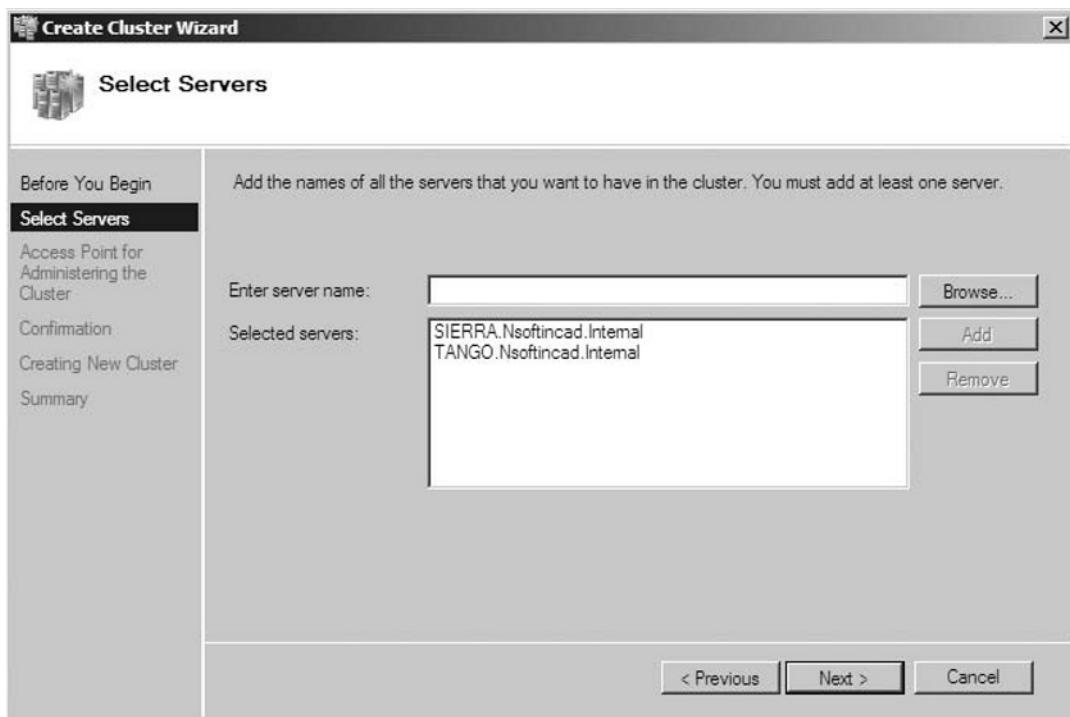
13. Once completed, review the generated **Failover Cluster Validation Report**.
14. Resolve any issues identified in the report, prior to proceeding to the Cluster Creation process in the next step (see Figure 7.14).

**Figure 7.14** 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 7.15)

**Figure 7.15** 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 7.16).
19. Select **Next** to proceed.

**Figure 7.16** Create Cluster Wizard—“Select Servers” Page

### TEST DAY TIP

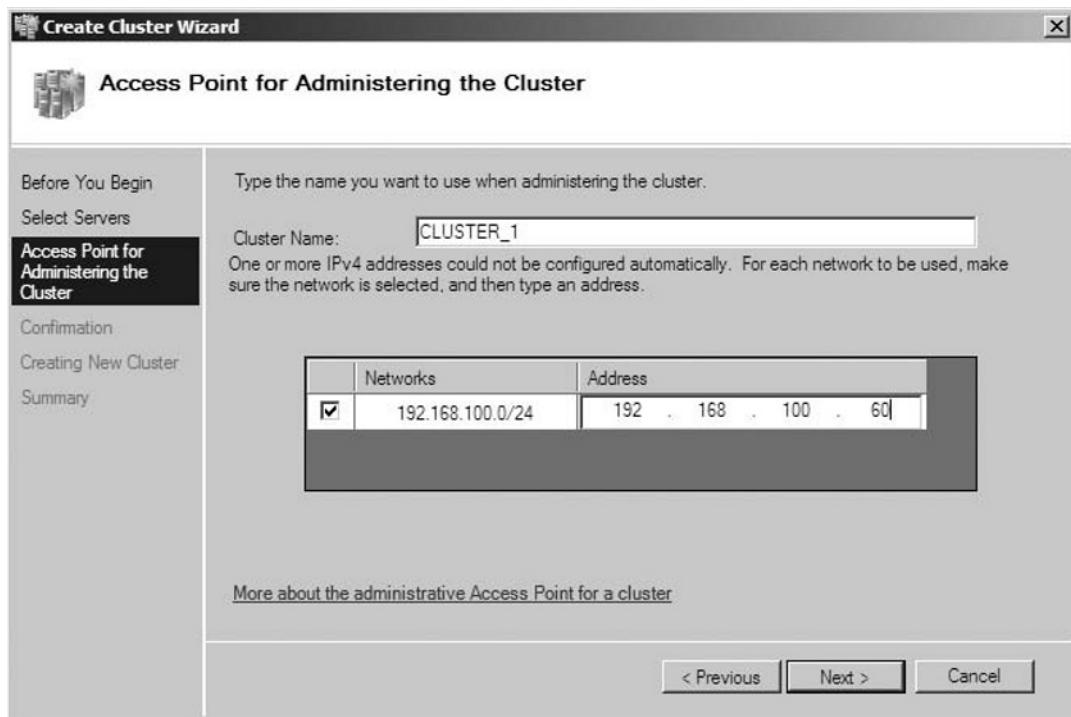
If the installation of the **Failover Cluster Feature** has not been completed on each of the subject servers, they will report as being *Unreachable*.

### NOTE

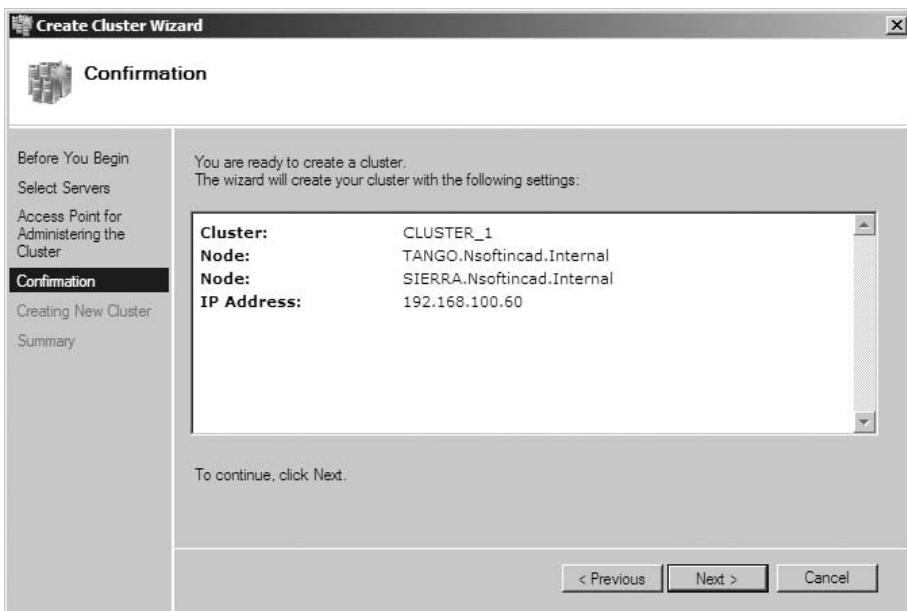
If Windows Firewall Protection is configured to block Remote Procedure Calls on the target node servers, this will also cause them to report as being *Unreachable*.

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 7.17.

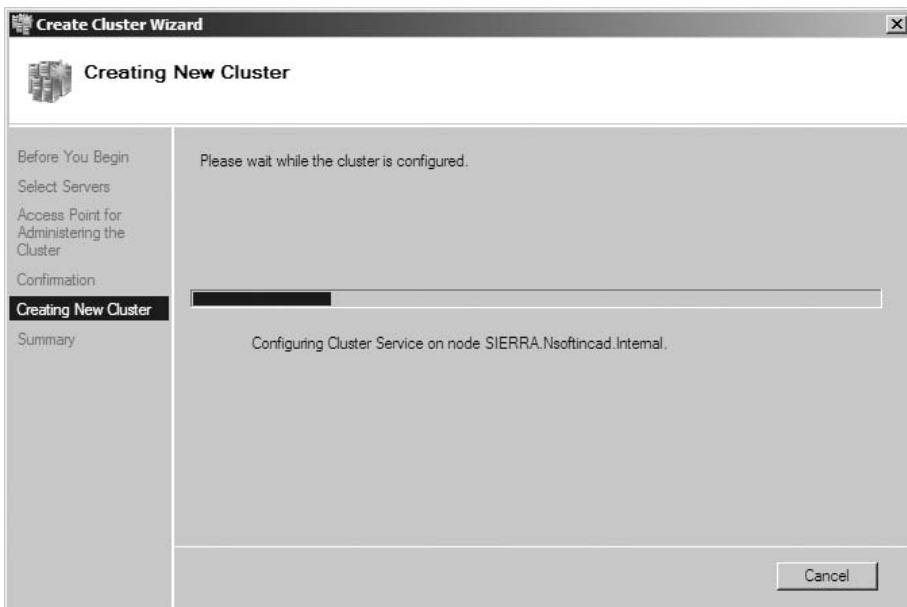
**Figure 7.17** Create Cluster Wizard—“Access Point for Administering the Cluster”



22. On the **Confirmation** page confirm all Cluster Creation Selections.
23. Select **Next** to proceed (see Figure 7.18).

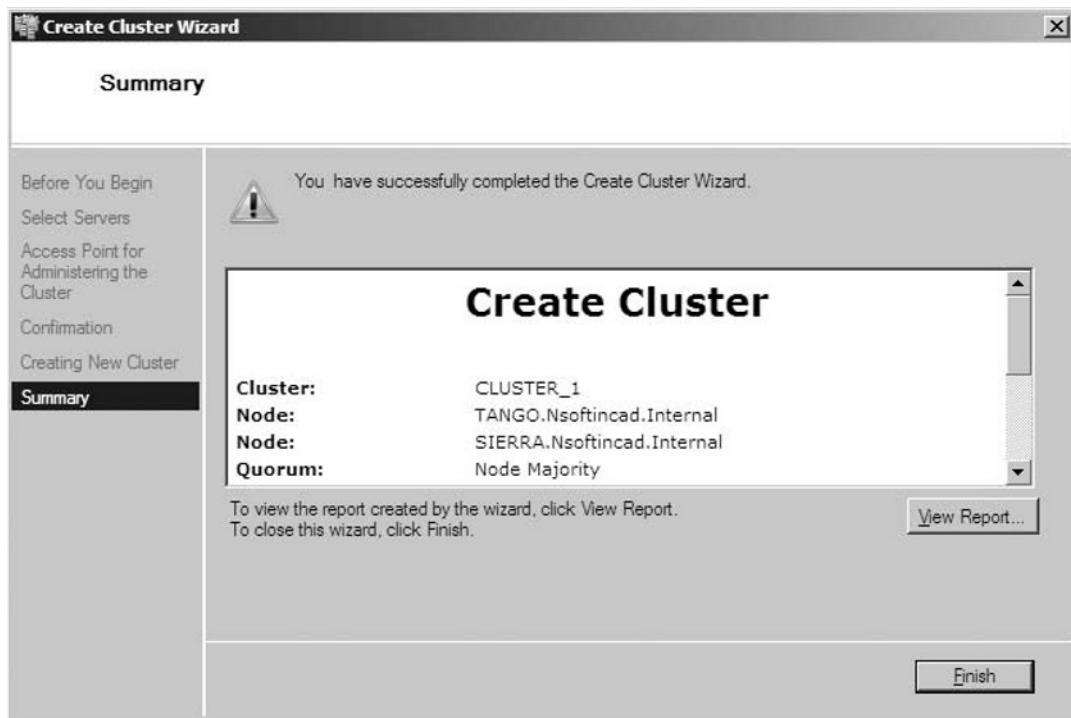
**Figure 7.18** Create Cluster Wizard—“Confirmation” Page

24. The **Creating New Cluster** process will take a few minutes to run (see Figure 7.19).

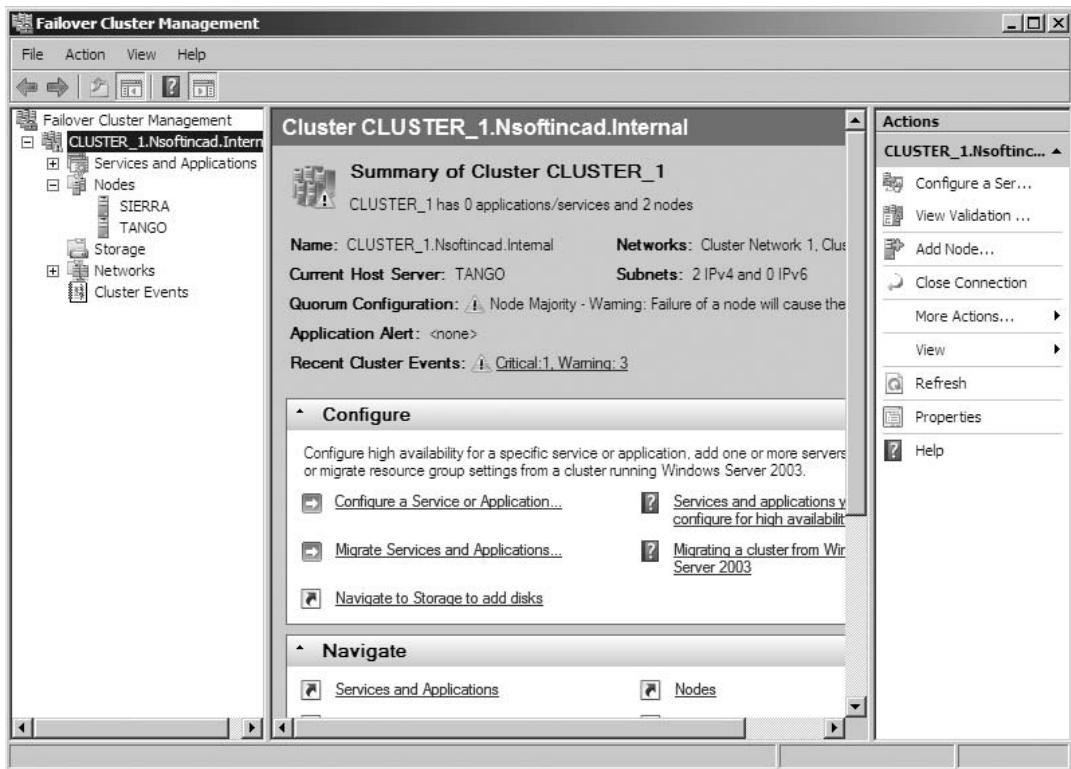
**Figure 7.19** Create Cluster Wizard—“Creating New Cluster” Page

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 7.20.

**Figure 7.20** Create Cluster Wizard—“Summary” Page



27. Select **Start | Administrative Tools | Failover Cluster Manager** to view the details of the newly created Cluster (see Figure 7.21).

**Figure 7.21 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 7.2

### 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.

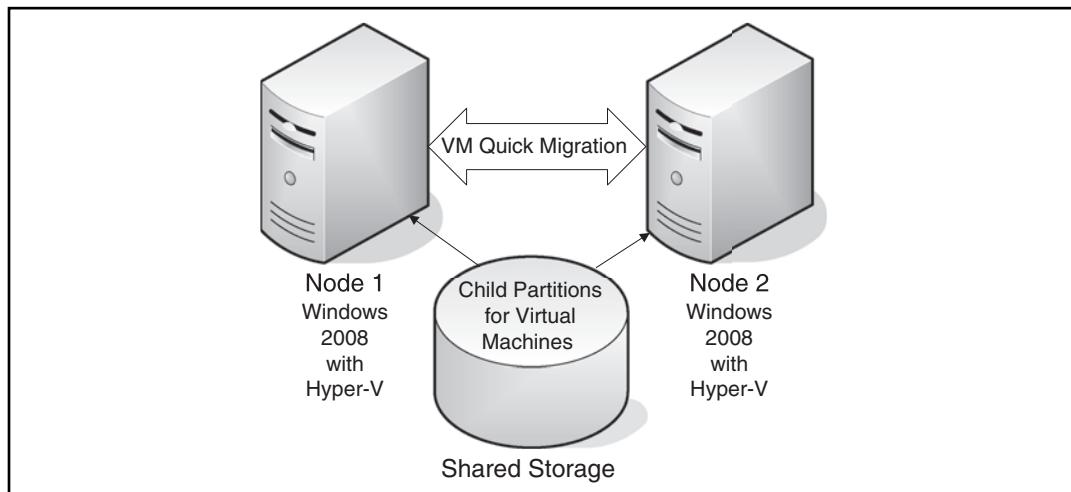
## Virtualization and High Availability

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 7.22). 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 7.22** 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:

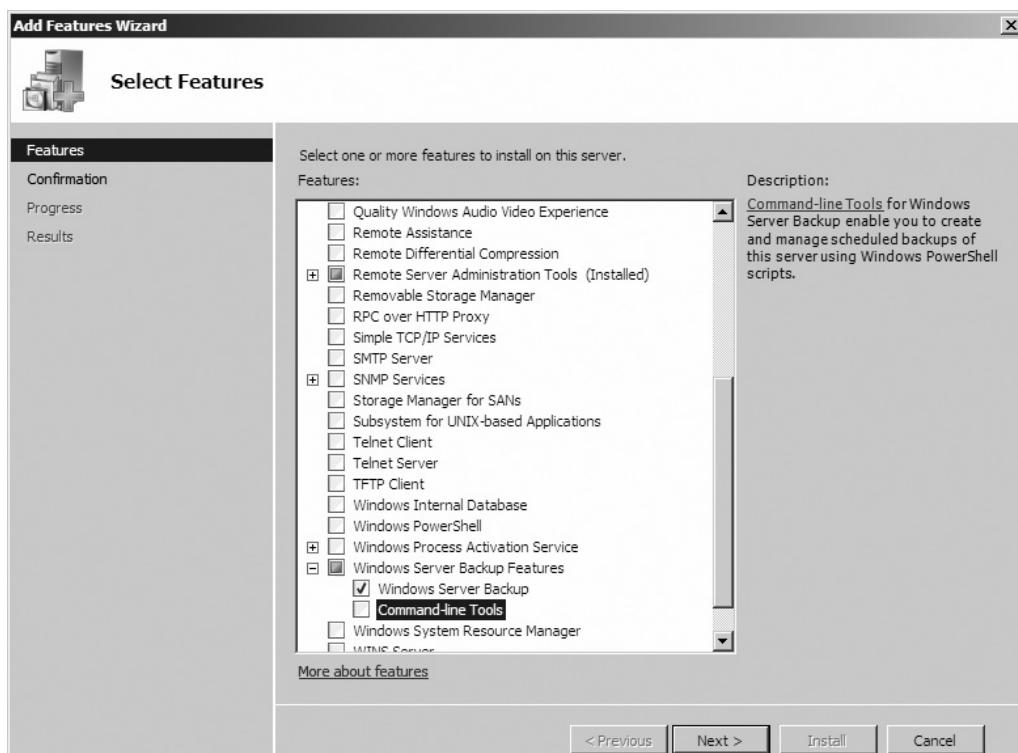
- **Initial Configuration Tasks Window** The Initial Configuration Tasks Screen that appears on the desktop after login provides the option to install Windows Server Backup by selecting **Add Features | Windows Server Backup Features | Windows Server Backup**.
- **Server Manager** Server Manager provides 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 7.3

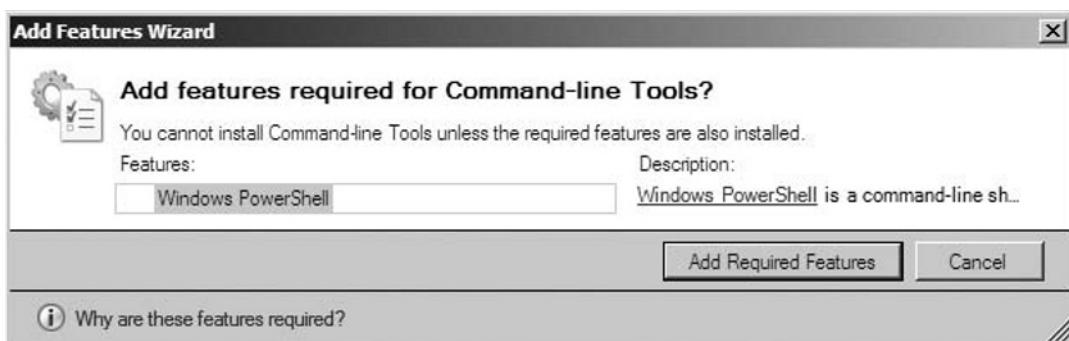
### INSTALLING THE WINDOWS SERVER BACKUP FEATURE ON A FULL INSTALLATION OF WINDOWS 2008 SERVER

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 7.23).

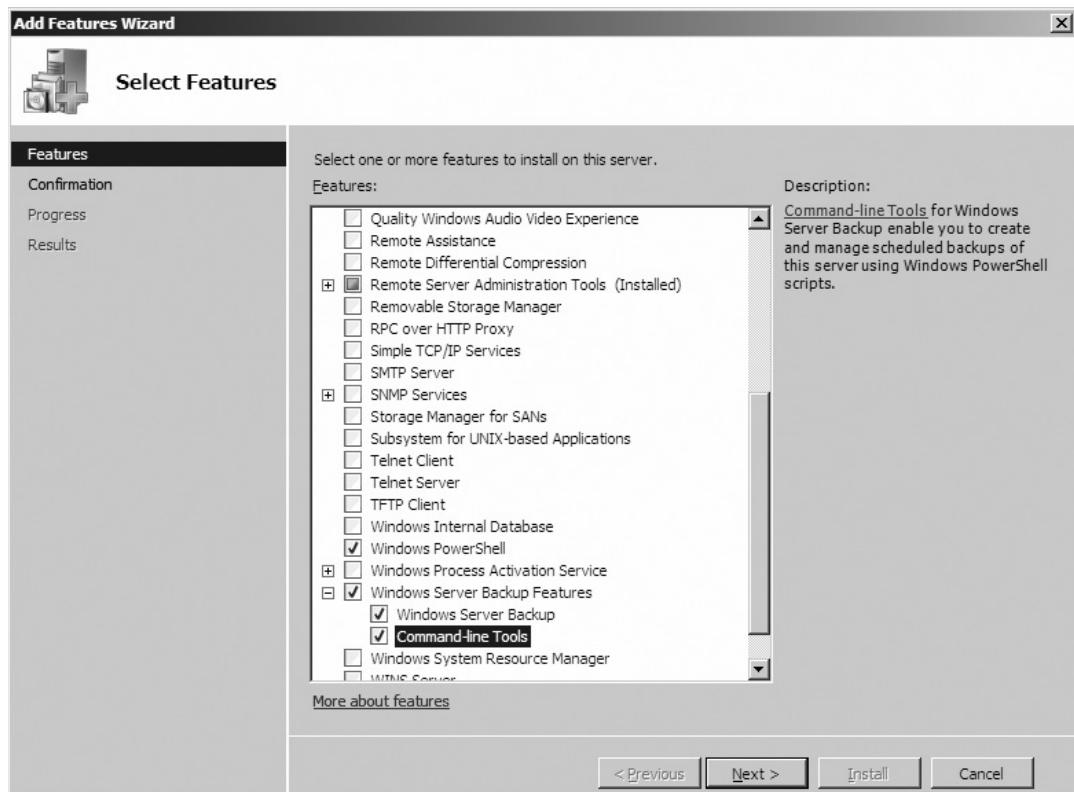
**Figure 7.23** Server Manager “Select Features” Wizard

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 7.24).

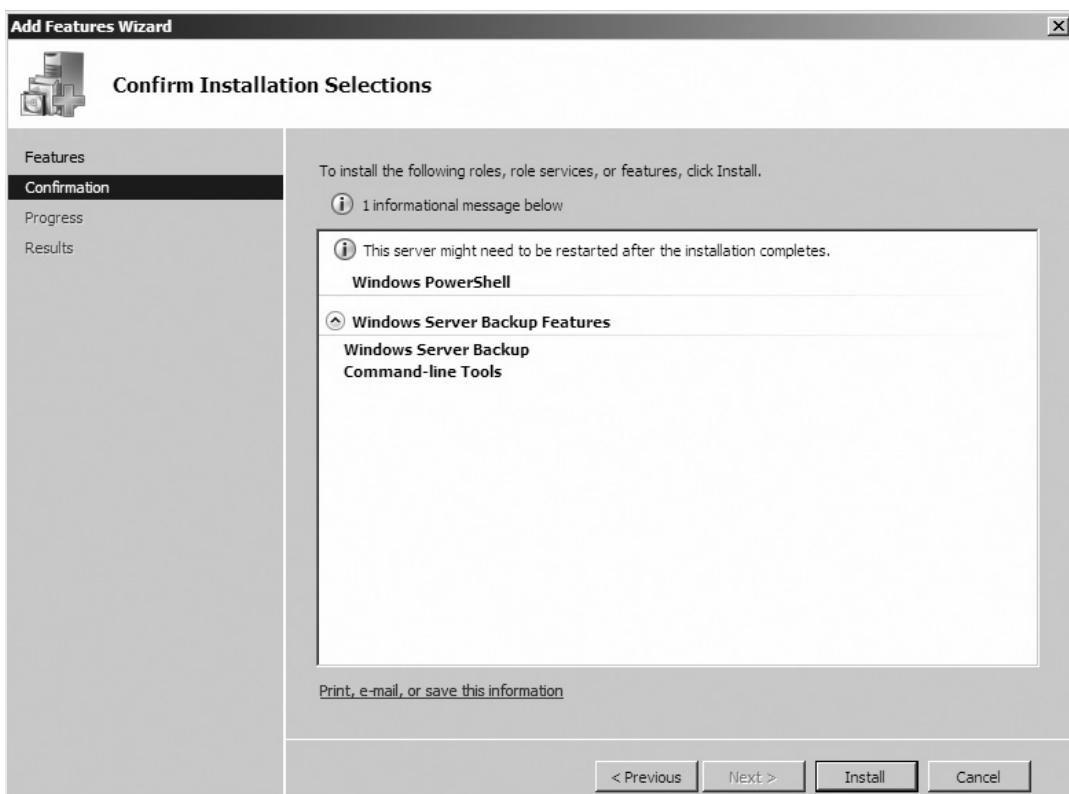
**Figure 7.24** Add Features Wizard “Add Features Required For Command-Line Tools?”

- Once the additional **Command Line Tools** option has been successfully added, select **Next** to continue (see Figure 7.25).

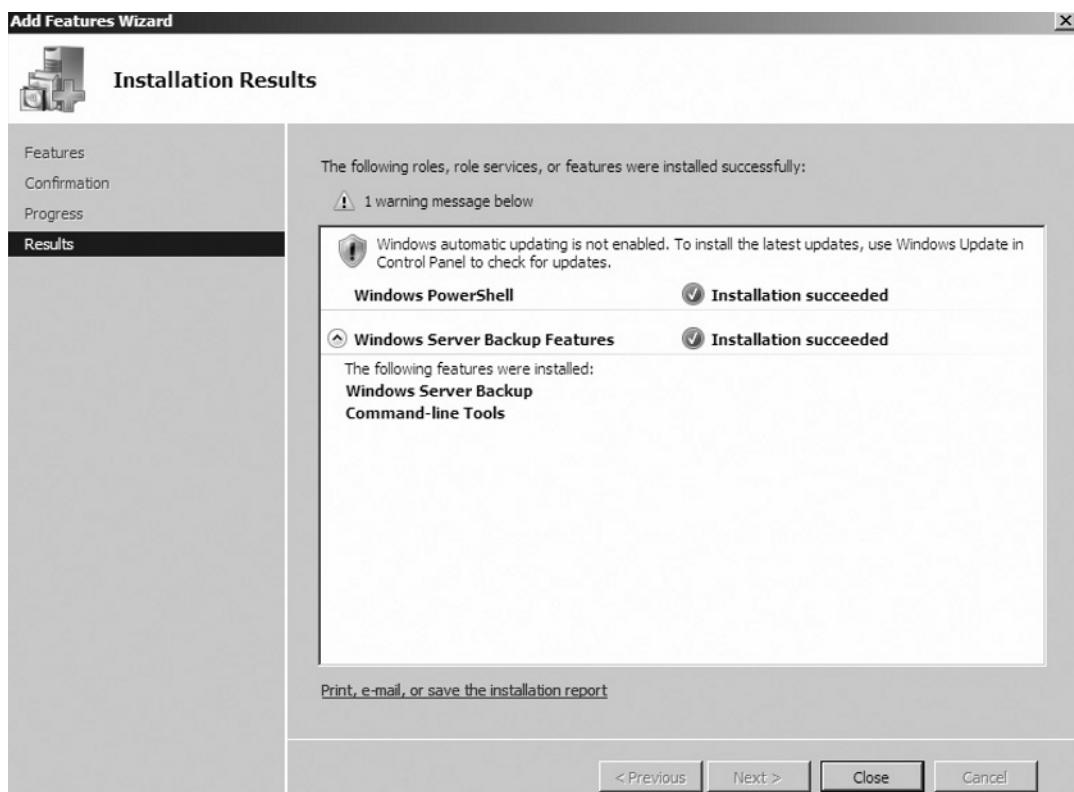
**Figure 7.25** Add Features Wizard “Select Features” Page



- In the **Confirm Installation Selections** page verify that the correct options have been chosen, and then select **Install** to proceed, as seen in Figure 7.26.

**Figure 7.26** Add Features Wizard “Confirm Installation Selections” Page

7. Once the installation has completed, select **Close** to complete the installation process (see Figure 7.27).

**Figure 7.27** Add Features Wizard “Installation Results” Page

- 
8. The Windows Server Backup Feature has now been successfully installed on your server.
- 

## EXERCISE 7.4

### 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**

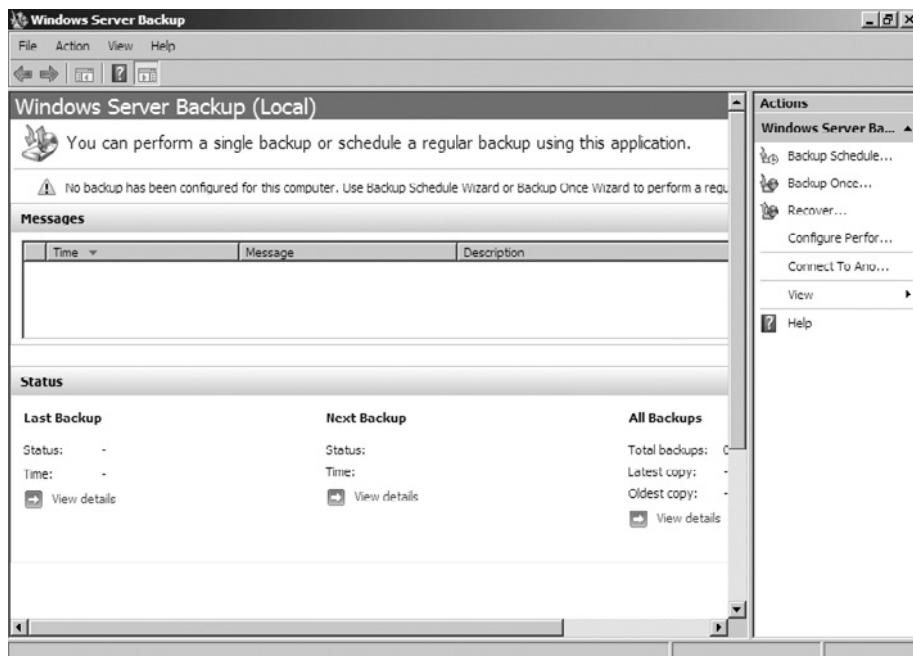
Windows Server Backup Utility provided with Windows 2008 Server does not support “Backup to Tape” functionality.

**TEST DAY TIP**

The Windows Server Backup Utility takes only one full snapshot of a volume. After that it's just differentials.

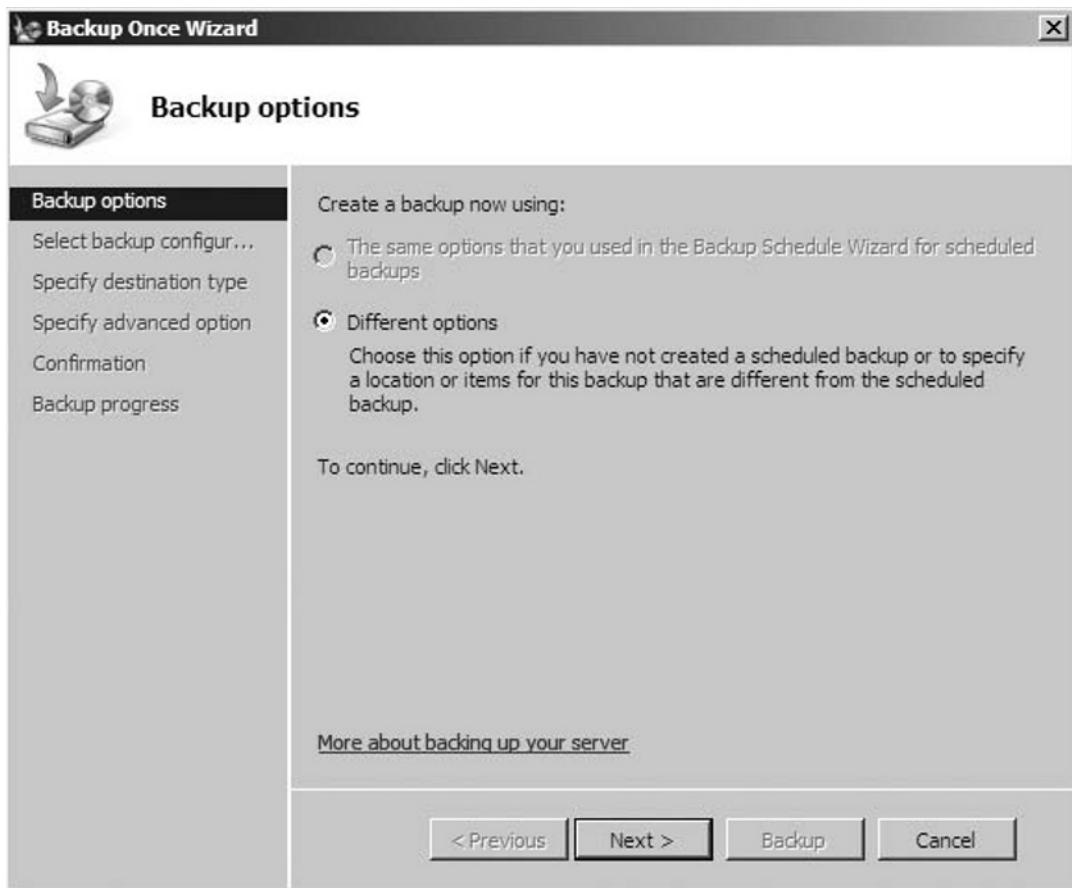
1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Windows Server Backup**.
3. In the **Actions** Pane to the upper right, select **Backup Once** (see Figure 7.28).

**Figure 7.28** 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 7.29).

**Figure 7.29** Backup Once Wizard “Backup Options”

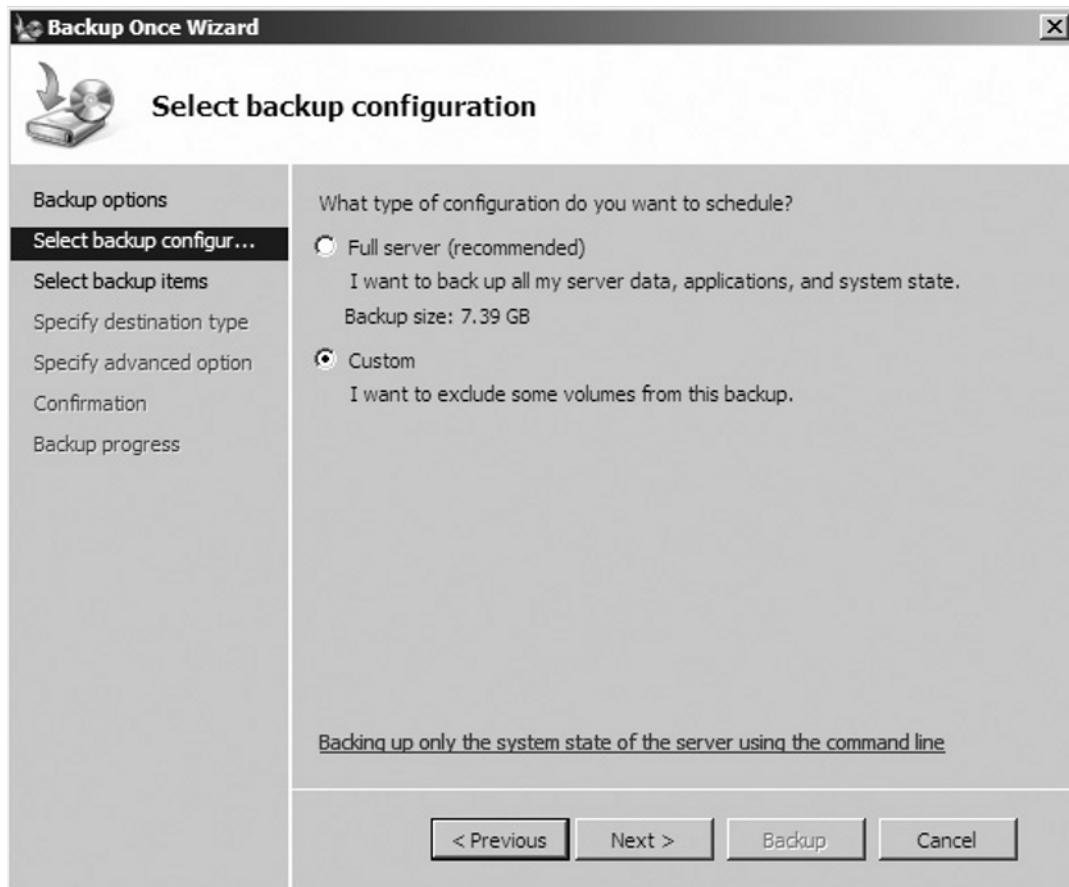


### NOTE

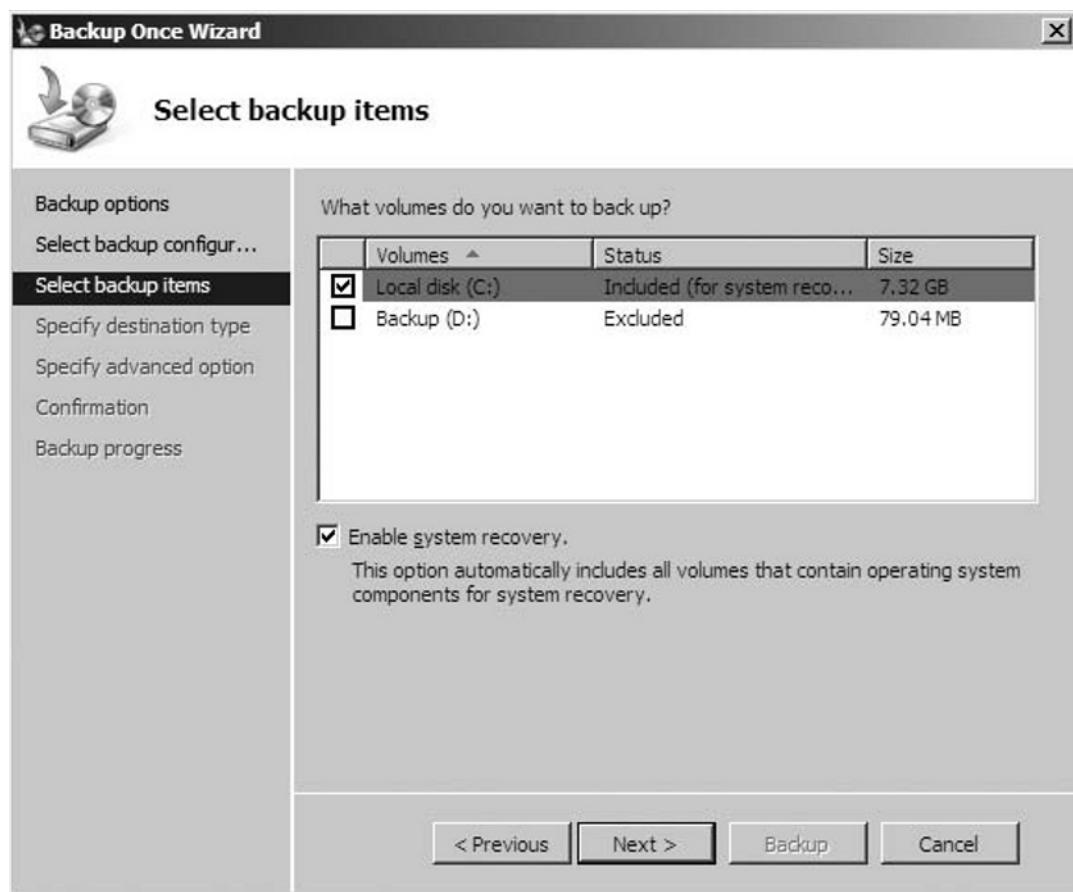
For subsequent backups the **same options** selection will be available, since there will then be selections available from previous backups that can be repeated if desired. On the first backup, **Different Options** is the only available selection since there are no historical settings available for selection at this point.

6. In the **Select Backup Configuration** Page select **Full Server**.
7. Select **Next** to proceed (see Figure 7.30).

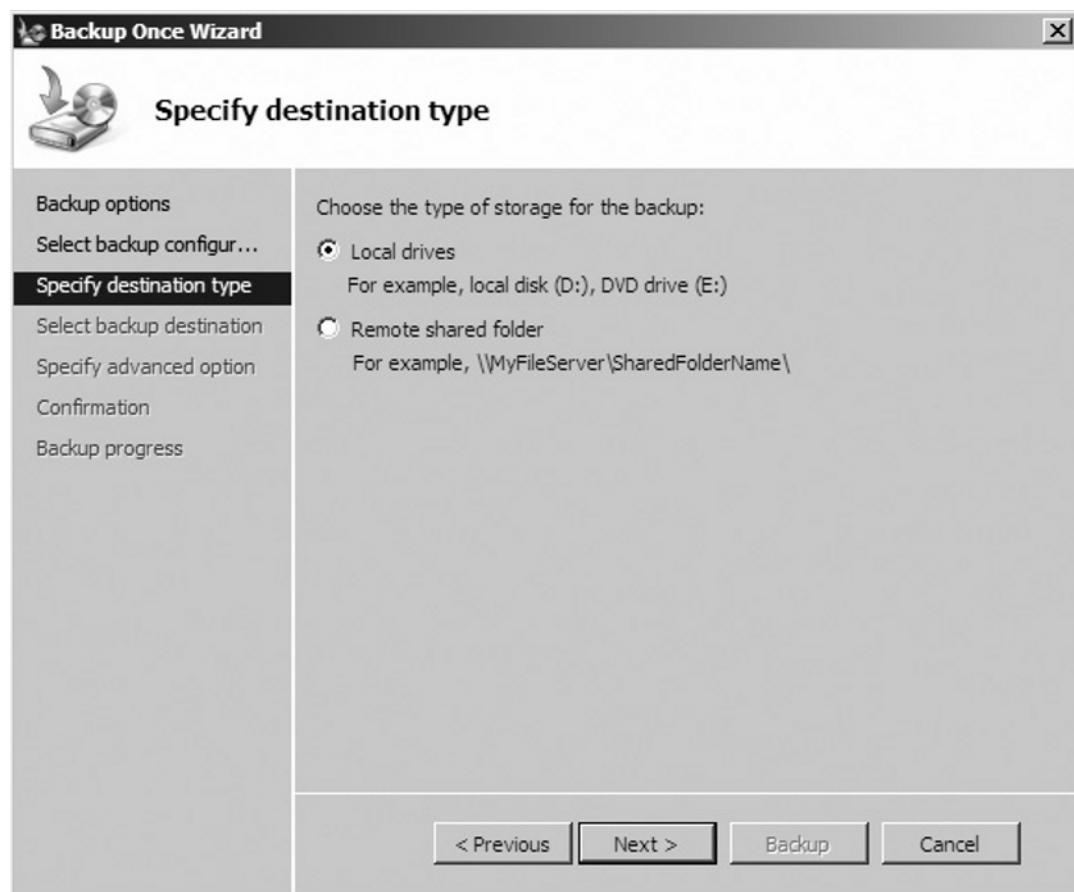
**Figure 7.30** Backup Once Wizard “Select Backup Configuration” Page



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 7.31).

**Figure 7.31** 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 7.32).

**Figure 7.32** 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 7.33).

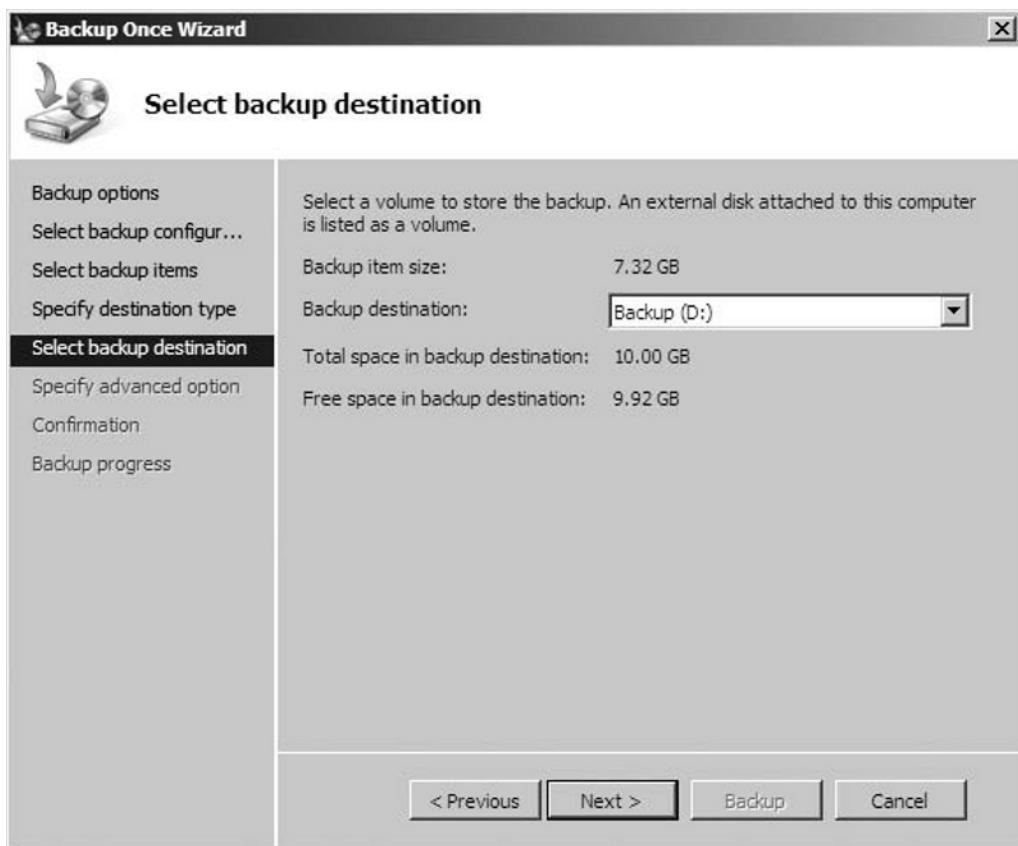
**TEST DAY TIP**

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**

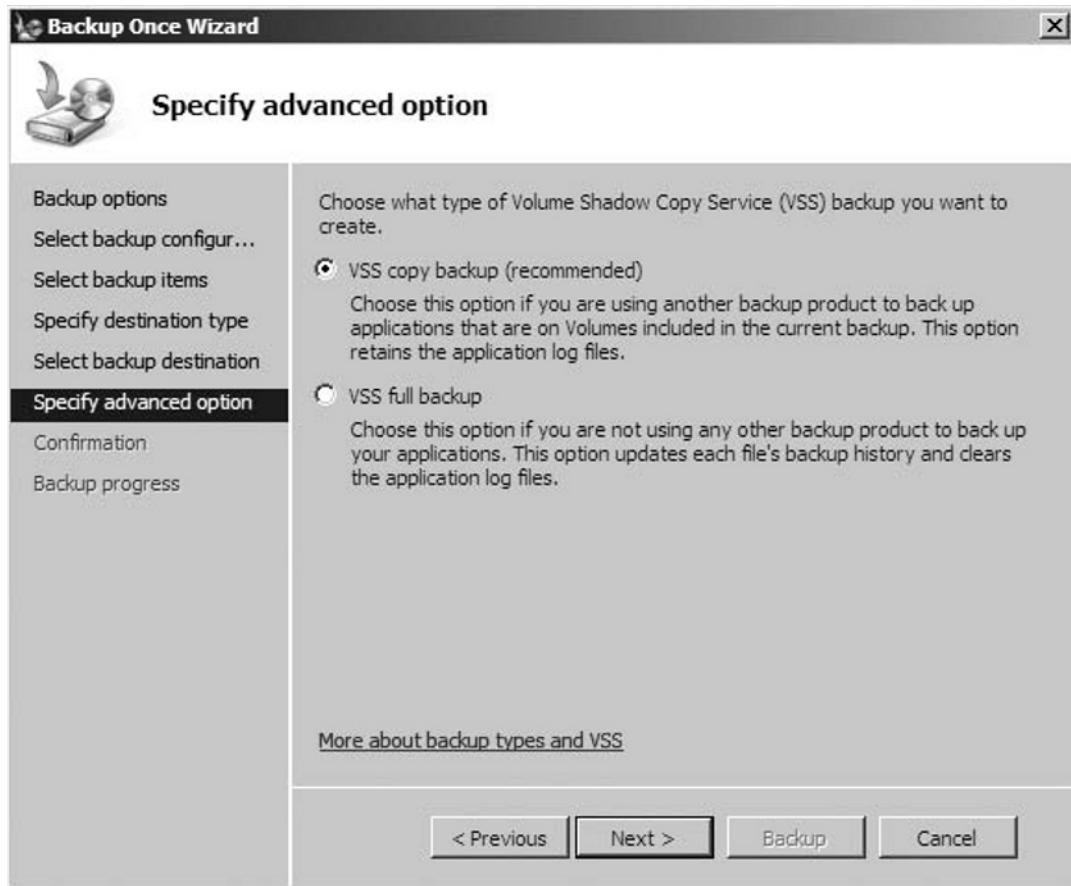
It is possible to override this limitation, by making a change in the registry. Microsoft's KB Article 944530 describes how to accomplish this change.

**Figure 7.33** Backup Once Wizard “Specify Backup Destination” Page

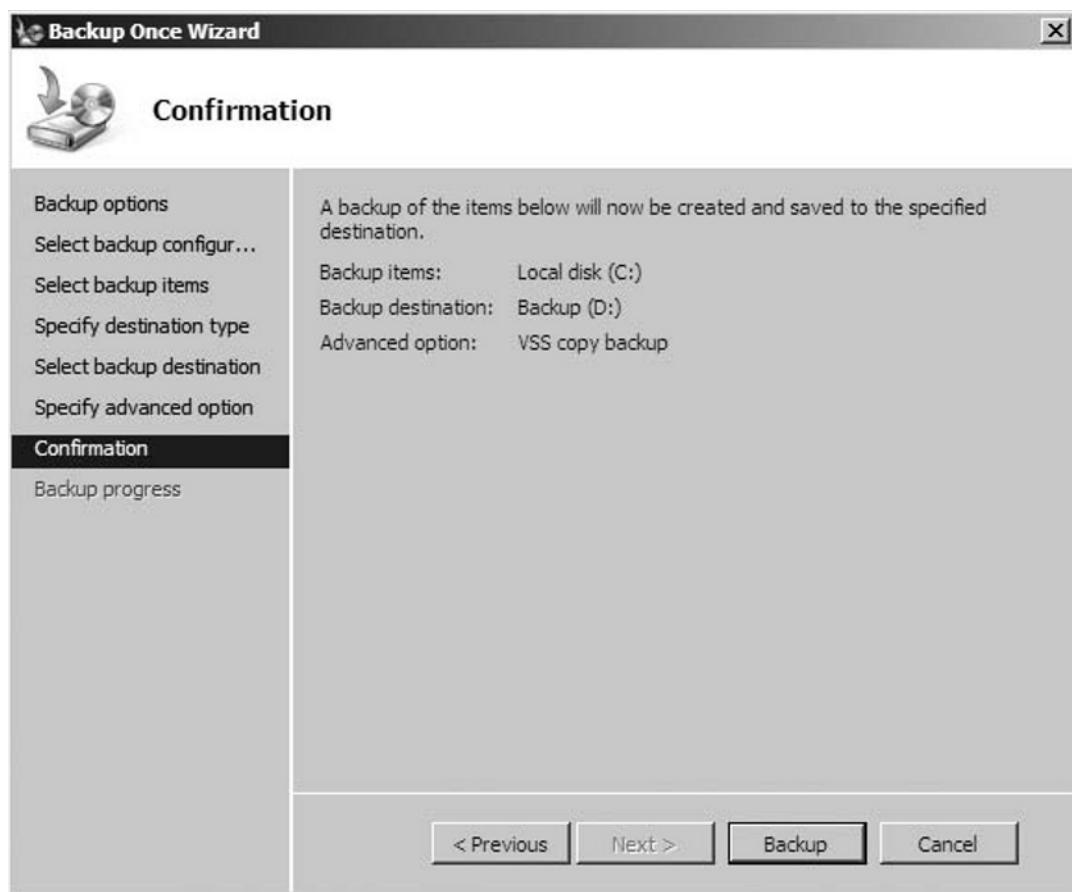


14. In the **Specify Advanced Option** page select **VSS Copy Backup**.
15. Select **Next** to proceed (see Figure 7.34).

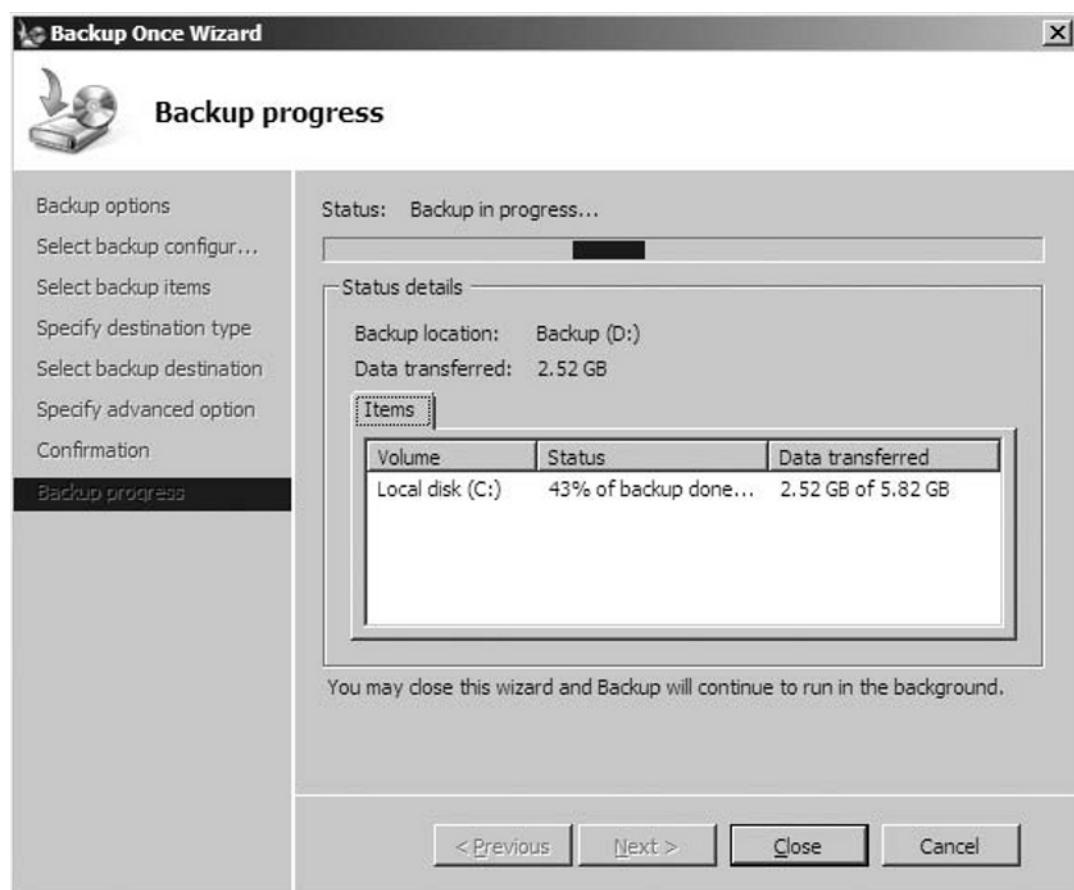
**Figure 7.34** Backup Once Wizard “Specify Advanced Option” Page



16. On the **Confirmation Page** review all selected options
17. Select **Next** to proceed (see Figure 7.35).

**Figure 7.35** 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 7.36).

**Figure 7.36** 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 7.5

---

#### PERFORMING THE OBJECT LEVEL RECOVERY OF INDIVIDUAL FILES USING THE WINDOWS SERVER BACKUP UTILITY ON A FULL INSTALLATION OF WINDOWS 2008 SERVER

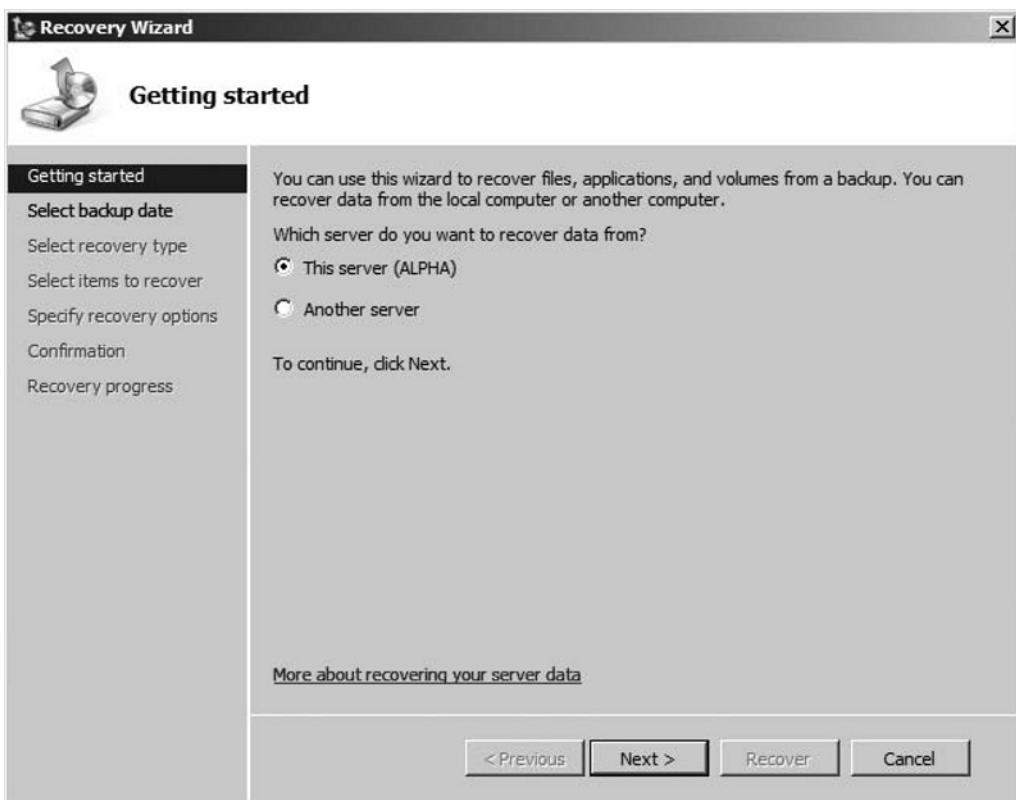
As a prerequisite this exercise assumes the pre-existence of a full installation of Windows 2008 Server, as well as completion of the previous procedure to install the Windows Server Backup feature, and availability of a valid backup of the subject files.

**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.

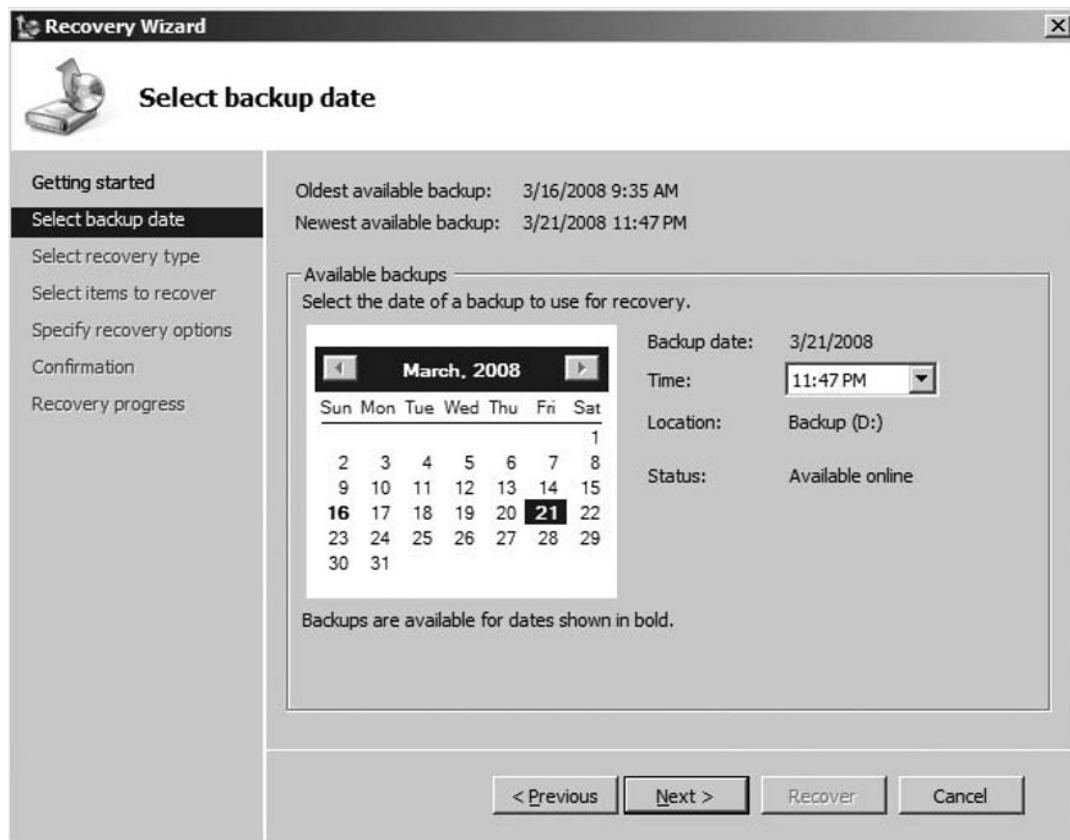
1. Log on to the Windows 2008 Server instance using an account possessing administrative privileges.
2. Select **Start | Administrative Tools | Windows Server Backup**.
3. In the Actions pane to the upper right, select **Recovery Wizard** (see Figure 7.37).

**Figure 7.37** Windows Server Backup—Recovery Wizard  
“Getting Started” Page



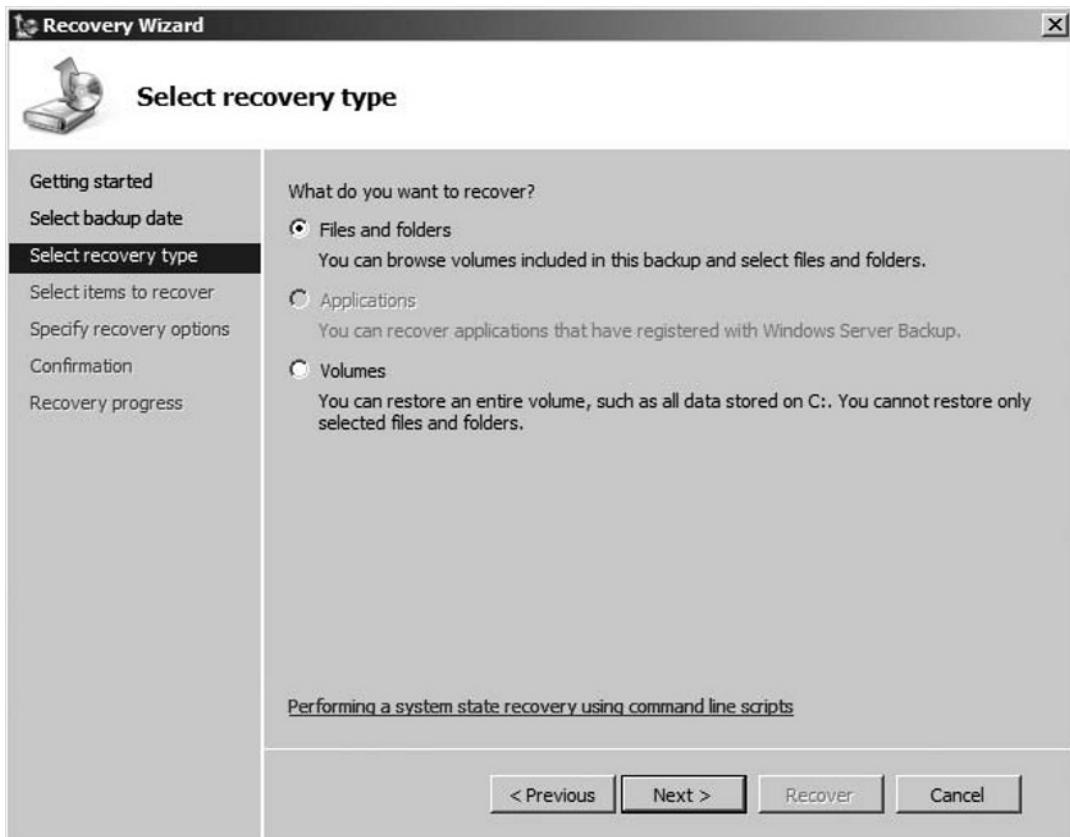
4. In the Select Backup Date page, choose the date for your backup (see Figure 7.38).

**Figure 7.38** Windows Server Backup—Recovery Wizard “Select Backup Date” Page



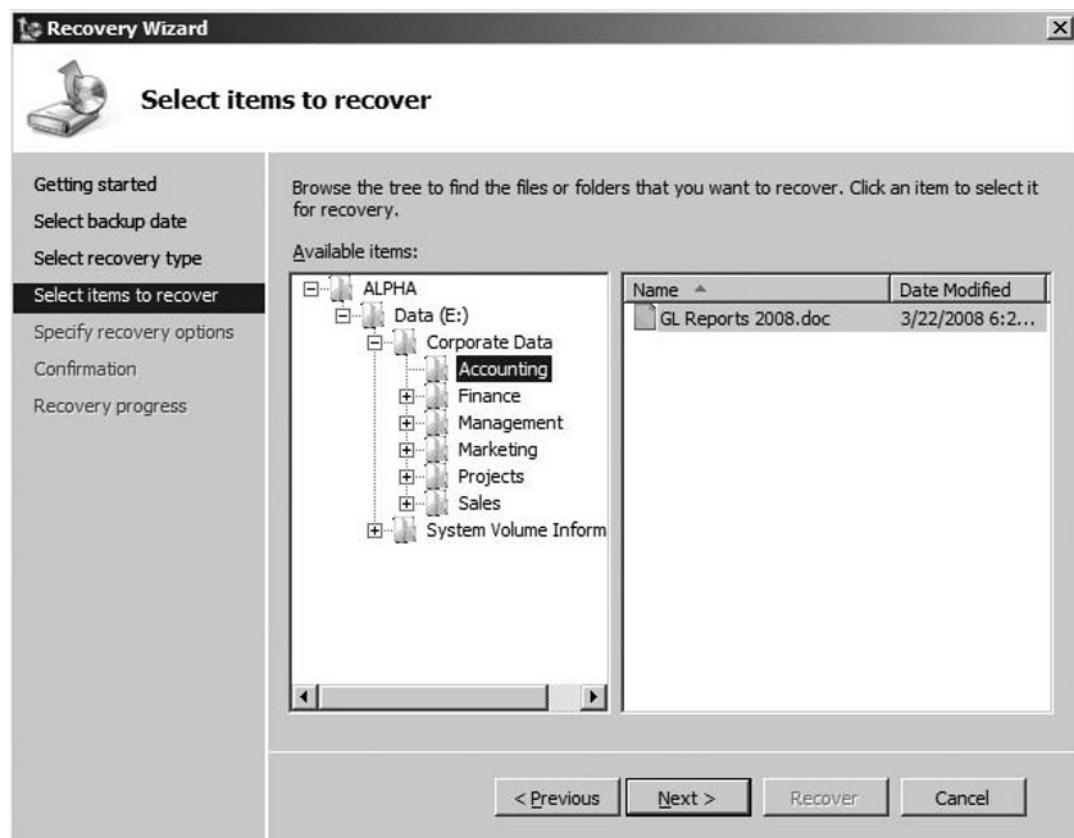
5. Select your recovery type (see Figure 7.39).

**Figure 7.39** Windows Server Backup—Recovery Wizard  
“Select Recovery Type” Page



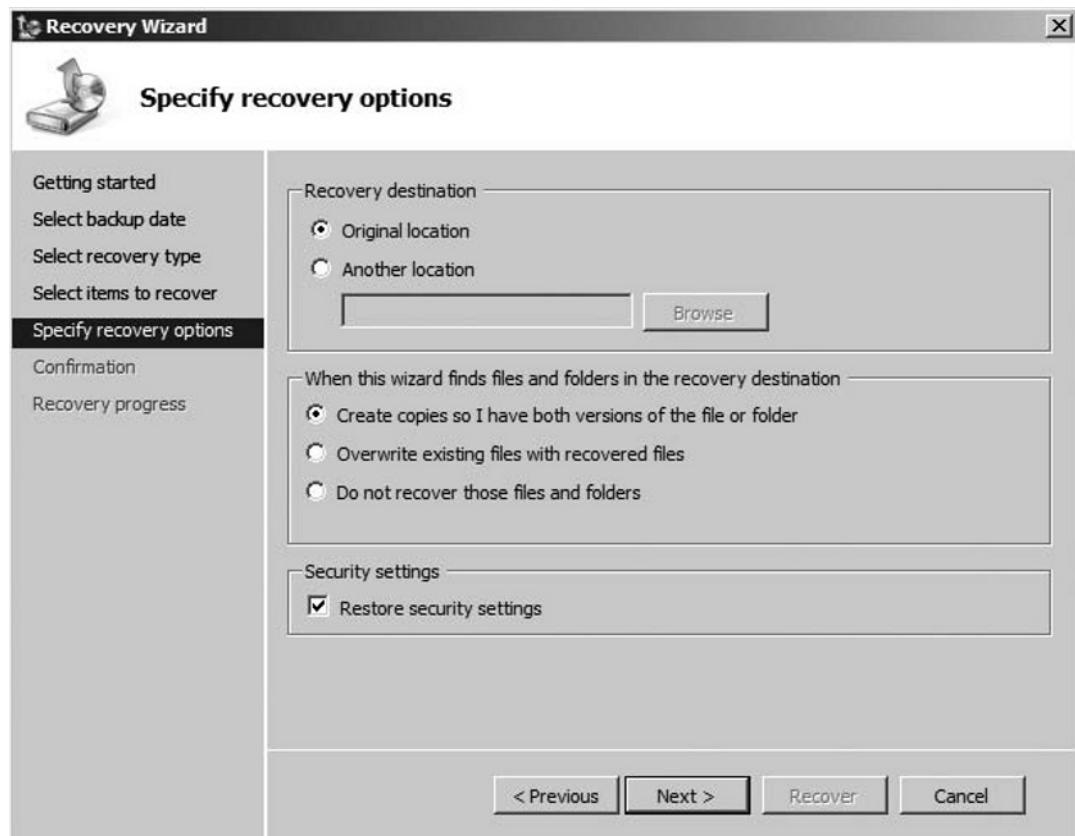
6. Select your items to recover (see Figure 7.40).

**Figure 7.40** Windows Server Backup—Recovery Wizard  
“Select Items to Recover” Page



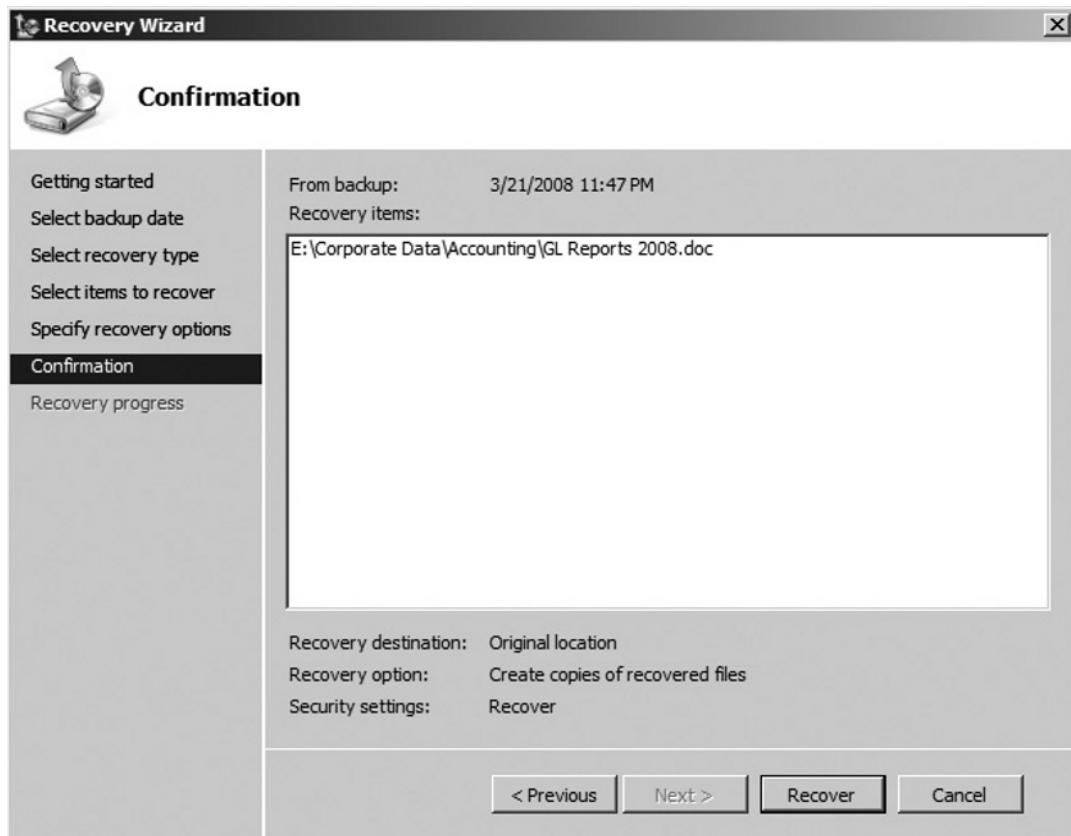
7. Specify your recovery options and click **Next** (see Figure 7.41).

**Figure 7.41** Windows Server Backup—Recovery Wizard “Specify Recovery Options” Page



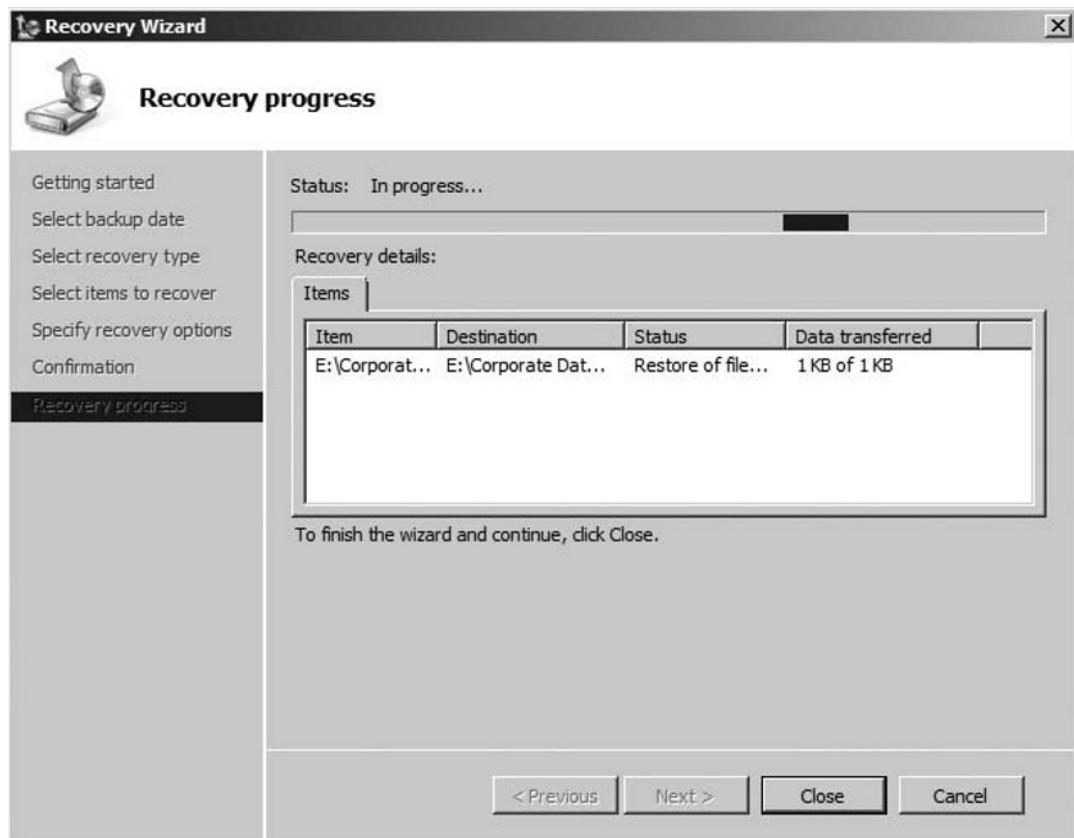
8. View the **Confirmation** page and then choose **Recover** (see Figure 7.42).

**Figure 7.42** Windows Server Backup—Recovery Wizard “Confirmation” Page



9. View the status on the **Recovery Progress** page (see Figure 7.43).

**Figure 7.43** 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>B, C</b> | 6. <b>D</b>    |
| 2. <b>B</b>    | 7. <b>A, B</b> |
| 3. <b>C</b>    | 8. <b>B, C</b> |
| 4. <b>A, B</b> | 9. <b>C, D</b> |
| 5. <b>B</b>    | 10. <b>C</b>   |

# **Appendix**

## **MCITP Exam 646**

### **Self Test Appendix**

# Chapter 1:

## Planning for Server Deployment

1. Your wireless network uses WEP to authorize users, but you also use MAC filtering to ensure that only preauthorized clients can associate with your APs. On Monday morning, you reviewed the AP association table logs for the previous weekend and noticed that the MAC address assigned to the network adapter in your portable computer had associated with your APs several times over the weekend. Your portable computer spent the weekend on your dining room table and was not connected to your corporate wireless network during this period of time. What type of wireless network attack are you most likely being subjected to?
  - A. Spoofing
  - B. Jamming
  - C. Sniffing
  - D. Man in the middle

Correct Answer & Explanation: **A.** You are the victim of a MAC spoofing attack whereby an attacker has captured valid MAC addresses by sniffing your wireless network. The fact that you have no other protection in place has made becoming associated with your APs an easy task for this attacker.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because jamming attacks are those in which high-power RF waves are targeted at a wireless network installation with the hope of knocking it out of operation by overpowering it.. Answer **C** is incorrect, because although your network has been sniffed previously to obtain the valid MAC address, you are currently being attacked using a spoofing attack. Answer **D** is incorrect, because a man-in-the-middle attack is one in which an attacker sits between two communicating parties, intercepting and manipulating both sides of the transmission to suit his or her own needs.

2. You are planning to upgrade to Windows Server 2008 and want to reuse existing servers only if they meet the recommended hardware requirements. During an assessment of your current servers you determine they all have a standard configuration of 80GB hard drive, dual 3.0GHZ processors, and

1GB of memory. Can you proceed to use the existing hardware? If not, what component must be upgraded?

- A. No, the hard drive must be upgraded to at least 100GB
- B. No, the memory must be upgraded to at least 2GB
- C. No, the CPU must be upgraded to at least 3.2 GHZ
- D. Yes, the current hardware configuration can be used

Correct Answer and Explanation: **B.** **B** is the correct answer because Microsoft recommends a minimum of 2GB of memory to install Windows Server 2008.

Incorrect Answers and Explanations: **A,C,D.** Answer **A** is incorrect because an 80GB hard drive is more than sufficient for Windows Server 2008 installation requirements. Answer **C** is incorrect because recommended minimum processor speed is 2Ghz. Answer **D** is incorrect because the server does require upgrading the memory before installing Windows Server 2008.

3. While planning your Windows Server 2008 deployment you determine you need to deploy two servers in your main office to support a SQL cluster. Which editions offer this capability? (Select all that apply)

- A. Standard Edition
- B. Enterprise Edition
- C. Web Edition
- D. Data Center Edition
- E. Itanium Edition

Correct Answers and Explanation: **B** and **D**. Both answers **B** and **D** are correct because both Enterprise Edition and Data Center Edition support Windows Server 2008 Clusters.

Incorrect Answers and Explanations: **A, C, and E.** Answers **A, C, and E** are incorrect because none of these editions can be used to support Windows Clusters.

4. Your security team has mandated that all new deployments of server operating systems must use BitLocker to provide disk level encryption. Which editions of Windows Server 2008 support disk encryption? (Select all that apply)
- A. Standard Edition
  - B. Enterprise Edition

- C. Web Edition
- D. Data Center Edition
- E. Itanium Edition

Correct Answers and Explanation: **A, B, D, and E.** Standard, Enterprise, Data Center, and Itanium Editions of Windows Server 2008 all support BitLocker drive encryption.

Incorrect Answers and Explanation: **C.** Answer C is incorrect because Web Edition does not support BitLocker Drive encryption.

5. Before upgrading to Windows Server 2008 you are required to provide a rollback plan to management. You must describe the process and tools used to perform the rollback in case of upgrade failure. What built-in tool can you use to rollback changes made by an upgrade to Windows Server 2008.
  - A. System Restore
  - B. Backup Wizard
  - C. Remote Assistance
  - D. Performance Monitor

Correct Answer and Explanation: **B.** Answer **B** is correct because the Backup Wizard provides a quick and easy way to perform a full or partial backup of your existing system.

Incorrect Answers and Explanation: **A, C, D.** Answer **A** is incorrect because System Restore is a feature in Windows XP and Vista client operating systems. Answer **C** is incorrect because Remote Assistance is used to remotely help other users to troubleshoot problems. Answer **D** is incorrect because Performance Monitor is not a backup utility. Performance monitor is used to capture and review various performance counters on the system.

6. You have decided to use Windows Deployment Services (WDS) to manage your operating system deployments. Before setting up WDS you want to ensure all infrastructure requirements are already met. What infrastructure services must you ensure are available before setting up WDS? (Select all that apply)
  - A. DNS
  - B. DHCP
  - C. RADIUS

D. Active Directory

E. IIS

Correct Answers and Explanation: **A**, **B**, and **D**. Answer **A** is correct because WDS requires the ability to perform name resolution on the network. Answer **B** is correct because systems that PXE boot must acquire an IP address to boot from the network.

7. You recently set up DHCP to supply IP addresses to all workstations on your network. All workstations at corporate headquarters, where the DHCP server is located, are receiving IP addresses properly. You have confirmed that servers with static IP addresses in the New Jersey office can connect to headquarters. However no workstations in the branch office in New Jersey are able to obtain IP addresses. What is the most likely cause of this problem?

- A. The WAN is currently down and the DHCP server is unreachable by the clients.
- B. The DHCP Server is offline.
- C. A DHCP Server must be set up in the Branch Office.
- D. The DHCP Server is not configured properly.

Correct Answer and Explanation: **C**. Answer **C** is correct because each network router typically cannot route DHCP requests or offers. You need a DHCP server on each network segment.

Incorrect Answers and Explanation: **A**, **B**, and **D**. Answer **A** is incorrect because servers with static IP addresses can communicate across the WAN. Answer **B** is incorrect because workstations in the main office are properly receiving DHCP IP addresses. Answer **D** is incorrect because workstations in the office are properly receiving IP addresses.

8. You want to deploy Network Access Protection (NAP) to ensure all client computers have current software updates installed before connecting to the network. Your clients consist of Windows 2000 Service Pack 4, Windows XP Service Pack 2, Windows XP Service Pack 3, and Windows Vista. Which clients must you upgrade before deploying NAP? (Select All That Apply)
- A. Windows 2000 Service Pack 4
  - B. Windows XP Service Pack 2
  - C. Windows XP Service Pack 3

- D. Windows Vista
- E. None of the clients need to be upgraded

Correct Answers and Explanations: **A** and **B**. Both Answers **A** and **B** are correct because Windows 2000 and Windows XP Service Pack 2 are not supported by Network Access Protection.

Incorrect Answers and Explanations: **C**, **D**, and **E**. Answers **C** and **D** are incorrect because Windows XP Service Pack 3 and Windows Vista are supported by NAP. Answer **E** is incorrect because Windows 2000 and Windows XP Service Pack 2 must be upgraded to be supported by NAP.

9. You are deploying Active Directory to provide directory services to your organization. Your Active Directory deployment will support 100 users and around 90 client workstations. The 90 users consist of three departments (accounting, human resources, and IT). All users and computers are located in one office and supported by a centralized IT Department of two Network Administrators. What is the best way to deploy Active Directory for this organization?
  - A. Deploy a single forest and domain for the organization.
  - B. Deploy a single forest with a parent domain and a child domain for each department.
  - C. Deploy a separate forest and domain for each department.
  - D. Deploy a separate forest for each department and use a single domain.
10. You are designing your domain controller deployment strategy and determine all branch offices need a domain controller at that location due to slow and sometimes unreliable WAN links. Your security team is somewhat concerned about placing a domain controller in the Toronto office as there isn't a very

secure location to physically store the server. What feature in Windows Server 2008 will allow you to place a domain controller in the Toronto office and ensure that no administrator accounts are stored on that server?

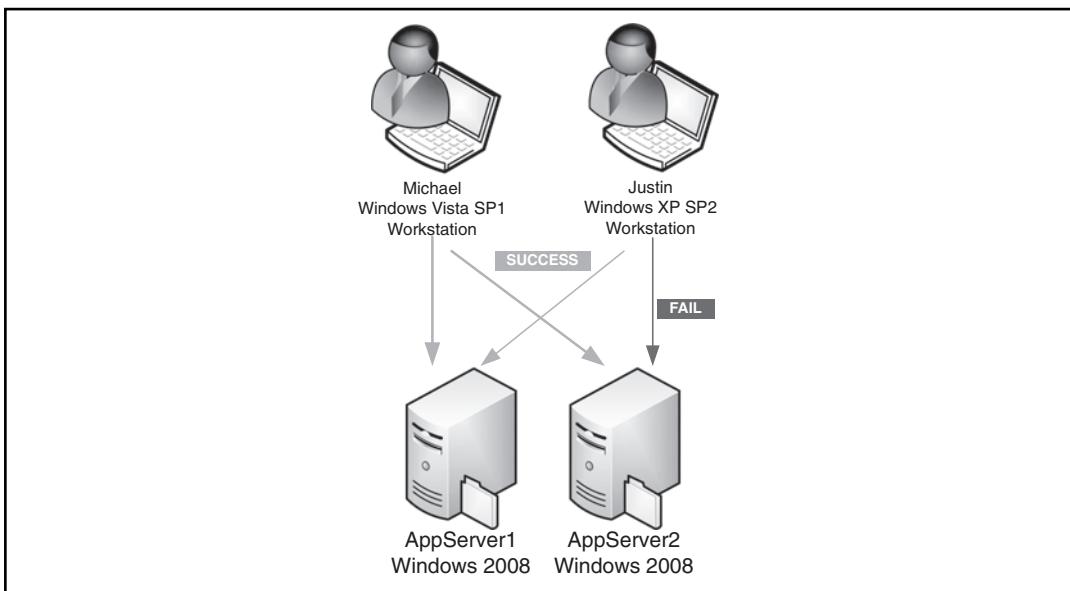
- A. Global Catalog
- B. Storage Policies
- C. BitLocker
- D. Read-Only Domain Controller

Correct Answer and Explanation: **D.** Answer **D** is correct because Read-Only Domain Controllers provide a read-only copy of Active Directory. Administrator accounts are never cached on Read-Only Domain Controllers.

Incorrect Answers and Explanations: **A**, **B**, and **C**. Answer **A** is incorrect because Global Catalog is a configuration option for Domain Controllers to provide a global collection of all objects in the forest. Answer **B** is incorrect because Storage Policies are a file storage feature in Windows Server 2008. Answer **C** is incorrect because BitLocker is not an Active Directory feature, but provides disk level encryption.

## Chapter 2: Planning for Server Management

1. Justin and Michael are administrators for a large financial firm. They are in the midst of a server deployment project and have decided to configure Remote Desktop for the eight new application servers they will be installing. All of the new servers will run Windows 2008 and will have a custom financial application installed. Once the first pair of servers has been installed with Windows 2008 and configured for Remote Desktop Justin and Michael decide to test their connectivity so that they can finish their application installs remotely. Michael is able to log on to both new servers, AppServer1 and AppServer2. Justin is able to successfully log on to AppServer1, however he is not able to successfully log on to AppServer2. Justin and Michael are both members of the Remote Desktop Users group (see Figure 2.37).

**Figure 2.37 Justin and Michael's Log-on Attempts**

Which of the following will allow Justin to authenticate against AppServer2 with the least amount of effort?

- A. Both Justin and Michael must be members of the Domain Administrators group.
- B. AppServer2 should have the Remote Desktop configuration adjusted to **“Allow connections from computers running any version of Remote Desktop (less secure)”**.
- C. Justin must upgrade his workstation to Windows Vista.
- D. Justin and Michael must install the MSTSC 6.0 on their workstations.

Correct Answer & Explanation: **B.** Since Justin is running Windows XP SP2 he would not have the ability to utilize Network Level Authentication. Even with RDC 6.0 installed he will not be able to connect to the server with the setting of **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)** configured. In order to connect to a Windows 2008 server that has been configured with **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)** Windows Vista or Windows Server 2008 would be required. So instead of upgrading his workstation Justin can simply toggle the radio button on the server to **Allow**

**connections from computers running any version of Remote Desktop (less secure)** which would then allow him to connect without requiring the Network Level Authentication component.

Incorrect Answers & Explanations: **A, C, D.** Answer **A** is incorrect, because Justin and Michael are already members of the Remote Desktop Users groups which are all the permissions they require in order to connect. Answer **C** is incorrect, because although this method would work since the RDC 6.0 client is native in Windows Vista it is by far the most amount of effort. Answer **D** is incorrect, installing the RDC 6.0 does not give Windows XP the ability to use Network Level Authentication. Also, only Justin needs a solution and this option mentions both Justin and Michael.

2. Your company is growing at a rapid pace and you find yourself presented with new lock-down settings from management every few weeks that need to be propagated out to different user departments. You have been creating a new GPO for each setting and then linking the new policies to the domain level or departmental OUs. Some users are starting to complain that it is taking a long time to log on and view their desktop. What is most likely the root cause in the logon slow down?
  - A. Your Active Directory domain controllers are too slow and need to be upgraded.
  - B. Users are downloading an increasing number of policies; therefore logon is slowed because the user workstations need to be upgraded since the HW is old and substandard.
  - C. Users are downloading an increasing number of policies; therefore logon is slowed while the machines wait for policies to process and the settings to apply.
  - D. Users are downloading an increasing number of policies; therefore logon is slowed due to insufficient bandwidth.

Correct Answer & Explanation: **C.** Creating many policies with few settings will increase logon time due to the overhead involved in connecting to download each policy. By creating fewer larger policies the number of trips to the DC for policy information is reduced and the machines can apply the settings in a much faster fashion.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, because a slow domain controller would result in problems during machine boot and authentication in many other places in the environment. This is still a possible

problem, but without more information it would be hard to pin it on the domain controllers. Answer **B** is incorrect, because although the client hardware plays a part in processing policies and in some cases could be a culprit, but since the users were not complaining before the new policies, the likeliness of the issue being with the workstation is slim. Processing Group policies should not be client intensive. Answer **D** is incorrect; bandwidth could be a culprit here, but by reducing the number of required trips across the wire you would reduce the need for additional bandwidth.

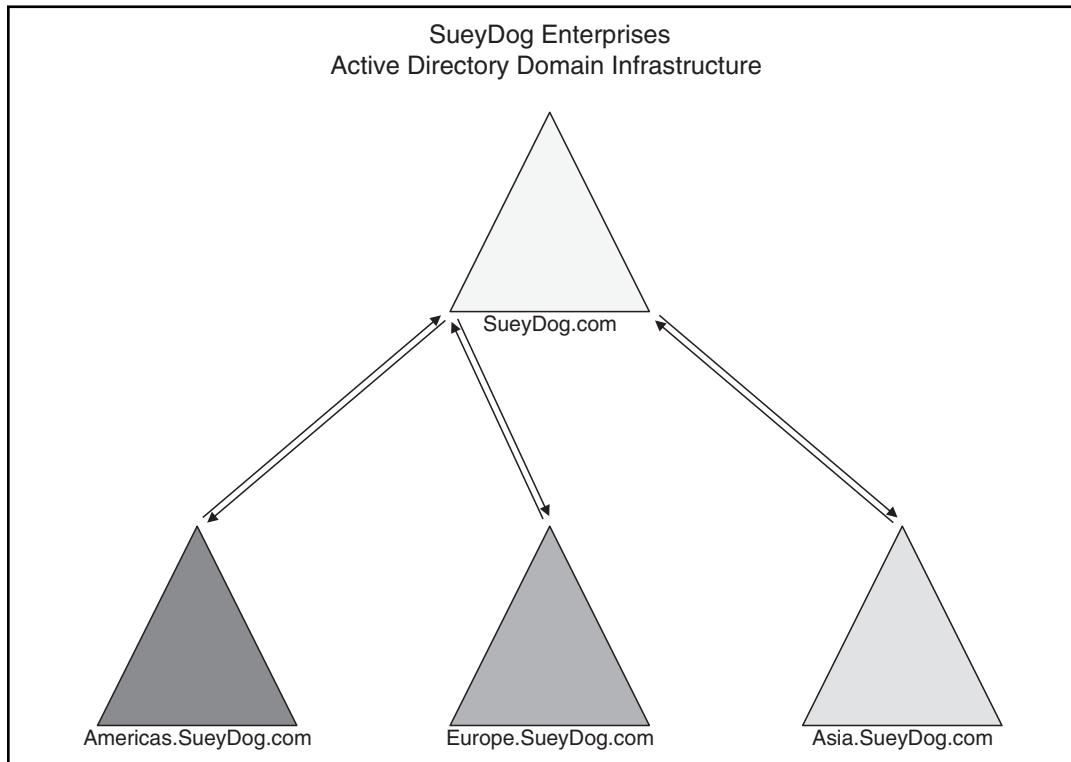
3. You need to create and apply a new Security Template for all of the database servers in your environment. Place the following steps in the correct order to accomplish this.
  1. Open a Custom MMC
  2. Add the Security Templates Snap-in
  3. Open Server Manager
  4. Edit your GPO
  5. Drill down to the Security Settings section of the GPO
  6. Right click the Security Settings section of the GPO and select to Import Policy
  7. Configure your new Security Settings
  8. Connect to the preferred storage location for Security Templates in your environment
  9. Create a new Security Template
  10. Save the Security Template
  11. Select the correct .inf file from the list of available files
  12. Browse to the location of the .inf files in your organization
    - A. 1,4,5,7,9,2,3,6,8,10,12,11
    - B. 1,2,8,9,7,10,3,4,5,6,11,12
    - C. 3,4,7,9,10,1,2,5,8,12,6,11
    - D. 3,4,9,5,6,10,8,11,2,7,1,12

Correct Answer & Explanation: **B**. This is the correct order of operations to accomplish this task.

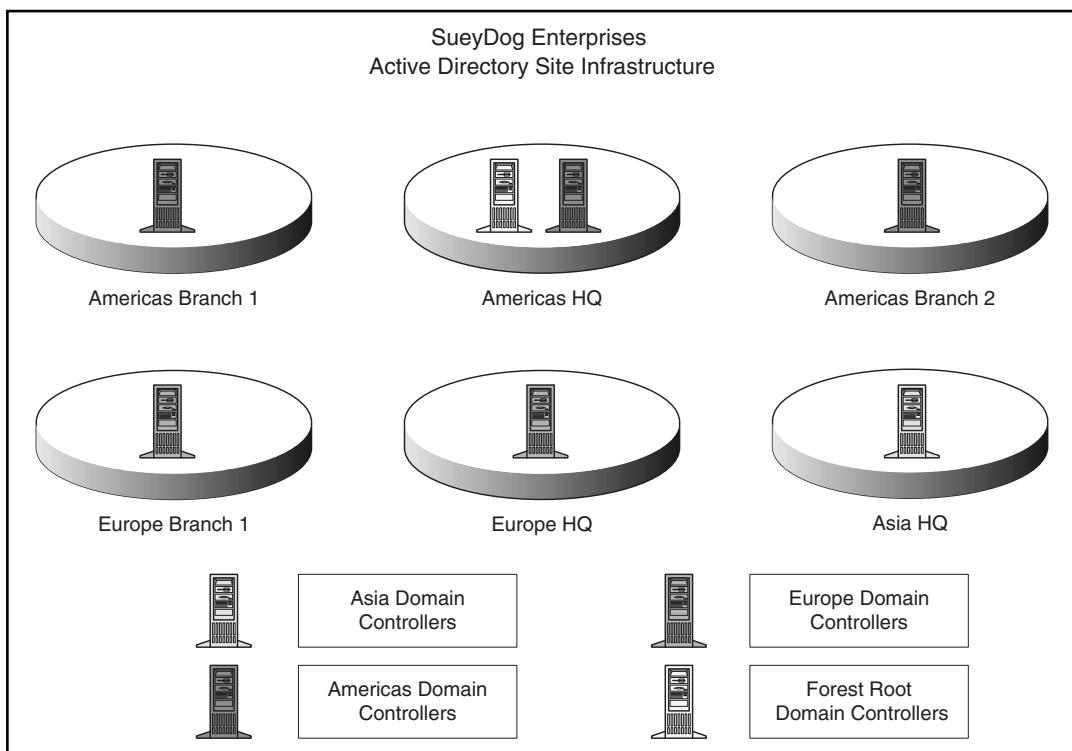
Incorrect Answers & Explanations: **A, C, D.** Answer **A, C, D** are incorrect, because these do not represent the correct order of operations for this task.

4. You are creating a new Group Policy that needs to be applied across two domains in your environment. The policy has approximately 350 settings. Your domain structure is depicted in Figure 2.38:

**Figure 2.38** SueyDog Enterprises AD Structure



You decided that to save time and administrative effort you will create the policy at the site level. The users that require the policy exist in America and Europe only. You link the policy to all of the Americas and Europe sites. Your Site structure is depicted in Figure 2.39.

**Figure 2.39** SueyDog Enterprises Site Infrastructure

The next day users begin complaining that log-on time has increased dramatically in Europe. Only some of the Americas users are complaining about slow log-on times. What is causing this problem?

- A. The domain controllers cannot handle such a large policy.
- B. The policy is too large and the client machines cannot handle such a large policy.
- C. Creating the policies at the Site level.
- D. The policy hasn't replicated to Europe or the branch offices in the Americas yet.

Correct Answer & Explanation: C. Creating a policy at the Site level stores the policy GPT on the DCs in the root of the forest. In this example DCs for the forest root only exist in the Americas HQ office. Users in that office are probably not experiencing a slow down. Users in any other office have to cross bandwidth in order to download the policy from the forest root DCs.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, because domain controllers are equipped to handle policies much larger than the one in this example. Answer **B** is incorrect, because although the policy may be larger than other policies in your environment this still isn't such a massive policy that it should bring clients' machines to a screeching halt. Answer **D** is incorrect, because Group Policies are part of the Domain context and will not replicate outside of the domain they are created in. So since the policy was created in the Forest Root, only Forest Root DCs will have a copy of the policy.

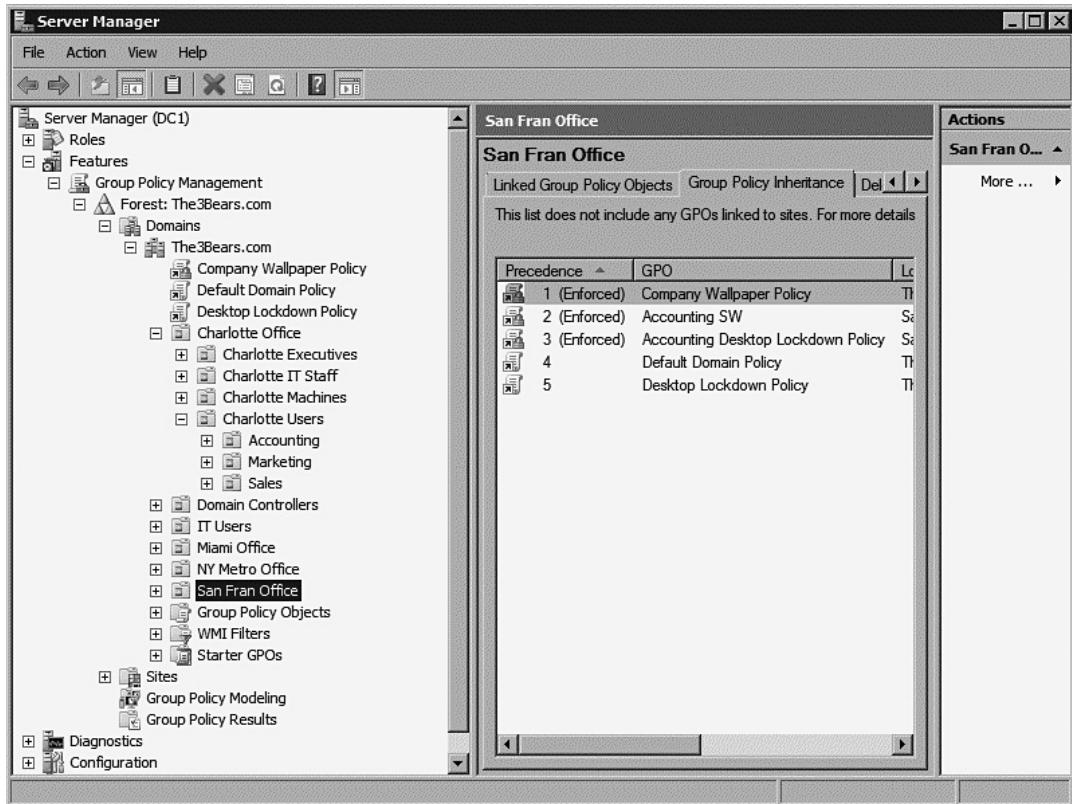
5. Darien is a new member of the Web Services team at your company. He is going to be responsible for running and testing scripts for an in-house home-grown application which requires a special application that is deployed via Group Policy. The first time he logs onto the domain he does not receive the software package. You verify that his user account is in the proper OU. What could be causing Darien not to receive the GPO with the software policy?
  - A. Security filtering has been enabled on the GPO and Darien is not a member of the proper group.
  - B. WMI filtering has been enabled on the GPO and Darien is not a member of the proper group.
  - C. Darien must be a local administrator on his machine in order to download a GPO with a software package in it.
  - D. Darien's user account has Block Inheritance configured on it and therefore he cannot download the policy.

Correct Answer & Explanation: **A.** Security Filtering utilized AD user and group objects to filter who is allowed to apply a GPO. If the default of Authenticated User has been removed from the GPO and the Web Services team group has been added, Darien will need to become a member of the Web Services team group in order to be able to apply the policy and receive the software package. Once he is added to the group he will have to log off and back on again in order to refresh his logon token.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because WMI Filtering targets machines, not users. Answer **C** is incorrect, because group policies are processed with System accounts and users do not require any special permission to apply them. Answer **D** is incorrect, because Block Inheritance is not configured at the user object level. It is configurable at the OU level.

6. Here is an image of your Active Directory Organizational Unit Architecture (See Figure 2.40).

**Figure 2.40 Active Directory Image**



As the administrator of The 3Bears Inc. you need all computers in the Charlotte office to be configured with a new Power Scheme. You create a Group Policy with the desired configuration and you need to select an OU to apply the settings. Which OU would you select to apply the policy?

- A. Charlotte Office
- B. Charlotte Executives
- C. Charlotte Machines
- D. Domain Level

Correct Answer & Explanation: **C.** Typically machines will be the targets for power settings and you can utilize Preferences to identify the type of machines through Targeting.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, this is the parent level OU and the parent level objects will trickle all policies down to the child OUs. Answer **B** is incorrect, because although Executive may be the primary owner of laptops if they also have a desktop and you apply this to the user there may be some inconsistency. Answer **D** is incorrect, because this would impact the entire domain with the policy.

7. SueyDog Enterprises will soon be deploying Microsoft Office Communicator into their environment. All of their domain controllers are running Windows Server 2008. Their administrator Matthew is attempting to prepare for the new product by creating a GPO and exploring the available settings. He creates a new policy and proceeds to expand each section of the policy looking for the section containing the Microsoft Office Communicator settings. He can't seem to locate the settings for Microsoft Office Communicator. What should Matthew do to gain the settings he seeks?
    - A. Download the appropriate ADM file and import it into the new GPO.
    - B. Install Microsoft Office Communicator on the domain controller to make the setting available.
    - C. Download the appropriate ADMX file and import it into the new GPO.
    - D. Download the appropriate ADM file and place it in the Central Store.
- Correct Answer & Explanation: **A.** By default Group Policies hold mostly operating systems settings. They can be customized with the use of either ADM or ADMX files. The ADM file format is imported directly into a GPO, the ADMX file format is placed into a Central Store that exists on SYSVOL.
- Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because installing a product does not make the settings for the product available in Group Policy. Answer **C** is incorrect, because although ADMX files could be utilized to gain access to the application's settings, these files are not imported into a GPO. They are placed in the Central Store and the Group Policy tools discover them there. Answer **D** is incorrect, because ADMX files belong in the Central Store, not ADM files.

8. Joey is going to be migrating his Lotus Notes environment into his newly established Windows Server 2008 forest. He has guidance on what he will require for Group Policy settings for the different teams and departments. He has not yet created his OU structure. How should Joey proceed in creating the required GPOs?
- Create Standalone GPOs.
  - Create the GPOs at the Domain level.
  - Create the GPOs at the Site level.
  - Wait to create the GPOs until the OU structure is in place.

Correct Answer & Explanation: **A.** Standalone GPOs are a way of staging GPOs so that when you are ready to link them they are ready to go. The advantage of a Standalone GPO is that it is not in use until linked so the settings can be readily changed on the fly without impacting users or computers.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because linking the GPOs at the Domain level would apply all the settings to all users and machines. The GPOs have specific target groups and linking all the policies at the domain would defeat their function. Answer **C** is incorrect, because linking at the Site is typically not recommended. Also, at this stage the Site structure might not be completed and to minimize the risk of the wrong user receiving a policy they should not be linked at the Site. Answer **D** is incorrect, because although the administrator can wait to create the GPOs until the OU structure is in place there isn't any reason to do. Standalone GPOs will fill the need for GPO creation.

9. How would you troubleshoot the following error message (Figure 2.41):

**Figure 2.41** Remote Desktop Connection Error Message



- In the Remote Desktop Connection client select **Options | Advanced** and adjusted your authentication choices.

- B. On the **System Properties | Remote** tab select “**Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**”
- C. On the **System Properties | Remote** tab select “**Allow connections from computers running any version of Remote Desktop (less secure)**”
- D. Both A and C

Correct Answer & Explanation: **C.** The error message occurs when a system incapable of running Network Level Authentication (like Windows XP) attempts to make a Remote Desktop connection into a machine configured with **Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)**.

Incorrect Answers & Explanations: **A, B, D.** Answer **A** is incorrect, because the setting regarding Network Level Authentication is a host side configuration, not a client side configuration. Answer **B** is incorrect, because enabling Network Level Authentication would not resolve the error. Answer **D** is incorrect, because although **C** is a correct answer, **A** is not.

10. You would like your users to be able to run a custom home-grown application in a centralized fashion. You install the application on your server and then add terminal services. You have a user attempt to connect using Remote Desktop and launch the application. The application does not work properly. How do you attempt to correct the problem?

- A. Uninstall the application, reinstall the application
- B. Install the TS Gateway role on the server
- C. Uninstall Terminal Services, uninstall the application, reinstall Terminal Services, reinstall the application
- D. Uninstall Terminal Services, reinstall the application, reinstall Terminal Services

Correct Answer & Explanation: **A.** When Terminal Services is installed any existing applications may need to be reinstalled in order to them to function properly.

Incorrect Answers & Explanations: **B, C, D.** Answer **B** is incorrect, because the TS Gateway role is for accessing the server via remote desktop through Internet-based connectivity. It wouldn't resolve any issues with installed

application. Answer **C** is incorrect, because uninstalling Terminal Services and reinstalling Terminal Services is not required. Answer **D** is incorrect, because the application needs to be reinstalled, not Terminal Services.

## Chapter 3: Monitoring and Maintaining Servers

1. Microsoft makes a free server-based patch solution available to customers for Microsoft current operating systems. This free server software is:
  - A. Microsoft Update
  - B. Windows Update
  - C. Windows Server Update Service
  - D. Microsoft System Center Essentials 2007

Correct Answer & Explanation: **C.** The only correct answer in this question is answer **C**, WSUS.

Incorrect Answers & Explanation: **A, B, D.** Microsoft Update and Windows Update are plausible answers but are not a server solution for the network infrastructure. Answer **D** is wrong because Microsoft System Center Essentials 2007 is a separate product that has to be purchased and licensed.

2. There are two ways Microsoft makes available to update the Windows Server 2008 operating system. These two types of operating system patch management include:
  - A. Microsoft Windows Server Update Services
  - B. Windows Update
  - C. Microsoft Update
  - D. Internet Explorer 7.0

Correct Answers and Explanation: **A, B.** The two correct answers are Microsoft Windows Server Update Services and Windows Update. Microsoft WSUS, clients would be setup to obtain updates from a WSUS server. When a client uses Windows Update—the client would connect to Windows Update website and download the updates directly from Microsoft.

Incorrect Answers and Explanation: **C, D.** Answer **C** is not correct terminology for Windows Update. Internet Explorer 7.0 is not required to obtain updates from the Windows Update site, so answer **D** is incorrect.

3. Your assistant Jim has just installed a new copy of Microsoft Windows Server 2008. You do not use Microsoft WSUS on your network. You instruct Jim to configure automatic updates through Windows Update on the newly installed server. Where could Jim configure this setting on the server?
- A. Computer Management
  - B. Server Management
  - C. Internet Explorer 7.0 Options
  - D. Windows Update Control Panel

Correct Answers and Explanation: **B, D.** The correct answers for this question would be Server Management and the Windows Update Control Panel.

Incorrect Answers and Explanation: **A and C.** Answers **A** and **C** are incorrect because there is no option in Computer Management or Internet Explorer 7.0 to set up Automatic Updates.

4. You wish to obtain the proper licensing for Microsoft Windows Server Update Service 3.0 SP1 for your network infrastructure. What are the proper licenses you must acquire to have a legal installation of WSUS?
- A. Internet Information Service 7.0
  - B. Windows Server 2008
  - C. None
  - D. Windows Server 2003 Advanced Edition

Correct Answer and Explanation: **C.** Microsoft Windows Server Update Service 3.0 SP1 is not a licensed product—it actually is provided free from Microsoft.

Incorrect Answers and Explanation: **A, B, and D.** You don't need to acquire licenses for Internet Information Server 7.0, Windows Server 2008 and Windows Server 2003 Advance Edition—this would make answers **A, B, and D** wrong.

5. When installing Microsoft Windows Server Update Services 3.0 SP1 on Windows Server 2008, we need to make sure that Internet Information Server 7.0 is configured with the proper components. Which of the following are components that are needed for a successful WSUS 3.0 SP1 installation?
- A. IIS Version 7 Management Compatibility
  - B. ASP.NET
  - C. Windows Authentication
  - D. IIS Version 7 Metabase Compatibility

Correct Answers and Explanation: **B, C.** The correct answer is ASP.NET and Windows Authentication, this makes **B** and **C** our correct answers.

Incorrect Answers and Explanation: **A, D.** Microsoft Windows Server Update Services 3.0 SP1 does require IIS Version 6 Management Compatibility and IIS Version 6 Metabase Compatibility—not version 7. This makes **A** and **D** incorrect.

6. What Microsoft operating systems can support a Microsoft Windows Server Update Service 3.0 SP1 installation for the server part of the installation?
  - A. Microsoft Windows Server 2008
  - B. Microsoft Windows Server 2003
  - C. Microsoft Windows Server 2000 Advanced Edition
  - D. Microsoft Windows 2003 with Service Pack 1

Correct Answers and Explanation: **A, D.** Microsoft Windows Server Update Service 3.0 SP1 can be installed on Windows Server 2003 Service Pack 1 or better and Microsoft Windows Server 2008. Therefore, answers **A** and **D** are correct.

Incorrect Answers and Explanation: **B, C.** WSUS does not support Windows Server 2003 with no service pack or no versions of Windows 2000 Server—so answers **B** and **C** are incorrect.

7. You are installing the Microsoft Windows Server Update Service 3.0 SP1 on a Windows 2008 Server. The server has a system drive that is formatted with FAT32 and a second drive that is formatted with NTFS and is compressed. The installation fails repeatedly. What do you need to do to make the installation work properly?
  - A. Uncompress the NTFS partition then continue installation.
  - B. Convert the FAT32 drive to NTFS and uncompress the NTFS partition—continue installation.
  - C. Run Windows Update.
  - D. Resize the NTFS partition and continue the installation.

Correct Answer and Explanation: **B.** Given this scenario answer B would be correct. To install WSUS, we would need to convert the FAT32 partition to NTFS and disable the drive compression.

Incorrect Answers and Explanation: **A, C, D.** WSUS does not support FAT32 or drive compression—so answers **A** and **D** are incorrect. Running Windows Update would not fix the installation problem for WSUS, so answer **C** is incorrect.

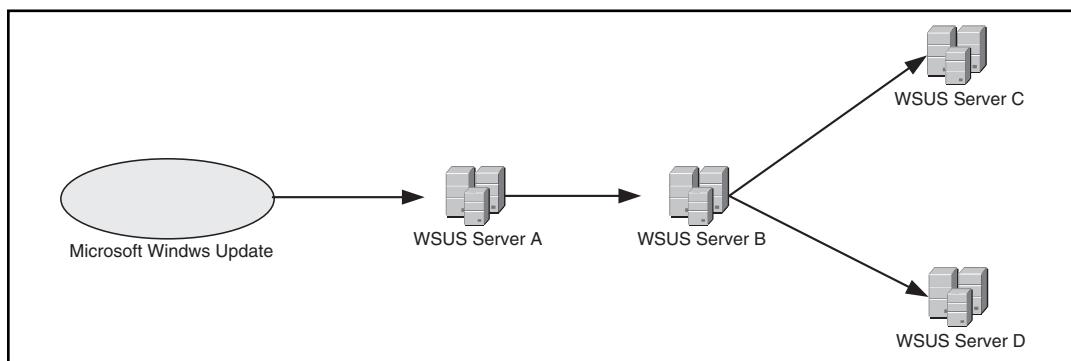
8. After installing Microsoft Windows Update Services 3.0 SP 1 on a Microsoft Windows 2008 Server you initiate the first synchronization. The WSUS directory grows in an excess of 20 GB. What would likely cause this to happen?
- A. The WSUS directory is on a FAT32 partition.
  - B. WSUS is installed on a compressed drive.
  - C. All languages are selected in the configuration.
  - D. The WSUS server is in replica mode.

Correct Answer and Explanation: **C.** The most likely option in this question is that all language updates are being downloaded to the WSUS server causing excessive space to be used. It is a good policy to only download the languages that are necessary for your implementation.

Incorrect Answers and Explanation: **A, B,** and **D.** WSUS cannot be installed on a FAT32 partition or compressed drive—so answers **A** and **B** are incorrect. If the server was in replica mode, this would not cause excessive drive space being used. This makes answer **D** incorrect.

9. Consider the WSUS server hierarchy shown in Figure 3.42; which server would be considered the primary upstream server?

**Figure 3.42** WSUS Server Hierarchy



- A. WSUS Server A
- B. WSUS Server B
- C. WSUS Server C
- D. WSUS Server D

Correct Answer and Explanation: **A.** The primary upstream server would be WSUS Server A; so answer **A** is correct.

Incorrect Answers and Explanation: **B**, **C**, and **D**. The other three servers would be considered downstream servers because their updates come from a primary upstream server in the network infrastructure. So answers **B**, **C**, and **D** are incorrect.

10. An upstream WSUS server shares updates with its downstream server or servers during synchronization, but not update approval status or computer group information. Downstream servers must be administered independently from the upstream server. What mode would the upstream server be in this design?
- A. Replica Mode
  - B. Independent Mode
  - C. Autonomous Mode
  - D. Server Core Mode

Correct Answer and Explanation: **C.** The correct answer would be **C**, autonomous mode. Autonomous mode shares updates with downstream servers, but not approval or computer group information.

Incorrect Answers and Explanation: **A**, **B**, and **D**. A server in replica mode shares approval and computer group information with downstream servers—so answer **A** is incorrect. Server Core mode is a type of Microsoft Windows 2008 Server installation that does not have the GUI installed, thus; answer **D** is incorrect. There is no such thing as independent mode—so answer **B** is incorrect.

## Chapter 4: Security and Policies

1. You want to set up a Routing and Remote Access Server using Windows Server 2008. Which of the following protocols are supported in Windows Server 2008?
- A. PPP
  - B. L2TP
  - C. PPTP
  - D. SSTP

Correct Answer & Explanation: **B**, **C**, and **D**. Layer Two Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and Secure Socket Tunneling Protocol (SSTP) are all supported in Windows Server 2008.

Incorrect Answers & Explanations: **A.** PPP (Point-to-Point Protocol) is not a VPN tunneling protocol.

2. You want to enable a Windows Server 2008 system to function as a Router between two networks. Which Role Service of the Network Policy and Access Services must you enable?
  - A. Network Policy Server
  - B. Network Routing Server
  - C. Routing and Remote Access Services
  - D. None of the above. Windows cannot be used as a router.

Correct Answer & Explanation: **C.** To use Windows Server 2008 as a router, you must enable the Routing and Remote Access Services, and verify that the routing feature is checked off as well during installation.

Incorrect Answers & Explanations: **A.** Answer **A** is incorrect, because NPS is used as a part of NAP and used for storing policies.

3. Network Access Protection (NAP) will only work with certain operating systems at the time of Windows 2008 Server release. What operating systems will NAP support?
  - A. Window XP
  - B. Windows XP Service Pack 3
  - C. Windows Vista
  - D. Windows Server 2008

Correct Answer & Explanation: **B, C, and D.** Natively, NAP will only support Windows XP SP3, Windows Vista, and Windows Server 2008. However, ISVs are developing clients for non-Windows clients.

Incorrect Answers & Explanations: **A.** Answer **A** is incorrect, because XP RTM, XP SP1, and XP SP2 do not support NAP.

4. Network Access Protection (NAP) can provide network protection to various types of network communications. Which of the following *will not* support NAP?
  - A. RRAS Connections
  - B. DHCP Supported Network
  - C. WINS Supported Network
  - D. IEEE 802.11B Wireless Network

Correct Answer & Explanation: **C.** WINS is a NETBIOS name resolution feature in Windows Server 2008, it does not support NAP.

Incorrect Answers & Explanations: **A, B, and D.** Answers **A** and **D** are incorrect, because all three of these technologies are supported by NAP.

5. The NAP Health Policy Server is responsible for storing health requirement policies and provides health state validation for the NAP Infrastructure. What Windows Server 2008 roles have to be installed for the NAP Health Policy Server to be configured?
  - A. Active Directory Domain Role
  - B. NPS Server Role
  - C. NAP Server Role
  - D. DHCP Server Role

Correct Answer & Explanation: **B.** In order for the NAP infrastructure to store policies, you must choose the NPS Server Role.

Incorrect Answers & Explanations: **A, C, and D.** Answers **A** and **C** are incorrect, because no such roles exist. Answer **D** is incorrect, since DHCP is used for dynamic IP assignment to client systems.

6. NAP Health Policies are a combination of settings for health determination and enforcement of infrastructure compliance. What are the sets of settings that make up the NAP Health Policies?
  - A. Connection Request Policies
  - B. Network Policies
  - C. Health Policies
  - D. Network Access Protection Settings
7. Encrypted Files and Folders are displayed with what color by default in Windows explorer?
  - A. blue
  - B. green

- C. grayed out
- D. red

Correct Answer & Explanation: **B.** Encrypted Files and Folders are displayed with the color green by default in Windows explorer

Incorrect Answers & Explanations: **A, C, and D.** Answer **A** is incorrect, because Encrypted Files and Folders are displayed with the color green by default in Windows explorer. Answer **C** is incorrect, because Encrypted Files and Folders are displayed with the color green by default in Windows explorer. Answer **D** is incorrect, because Encrypted Files and Folders are displayed with the color green by default in Windows explorer.

8. Where do you go to configure a secure connection between two nodes in the Windows Firewall with Advanced Security?
  - A. Connection Security Rules
  - B. Inbound Connections
  - C. Outbound Connections
  - D. Monitoring

Correct Answer & Explanation: **A.** A secure connection between two nodes is configured in the Connection Security Rules in the Windows Firewall with Advanced Security

Incorrect Answers & Explanations: **B, C, and D.** Answer **B** is incorrect, because a secure connection between two nodes is configured in the Connection Security Rules in the Windows Firewall with Advanced Security. Answer **C** is incorrect, because a secure connection between two nodes is configured in the Connection Security Rules in the Windows Firewall with Advanced Security. Answer **D** is incorrect, because a secure connection between two nodes is configured in the Connection Security Rules in the Windows Firewall with Advanced Security.

9. What are the two types of Security Associations that can be monitored in the Windows Firewall with Advanced Security?
  - A. Domain, Quick
  - B. Main, Quick
  - C. Public, Private
  - D. Public, Domain

Correct Answer & Explanation: **B.** Quick Mode and Main Mode are the two types of Security Associations that can be monitored in the Windows Firewall with Advanced Security.

Incorrect Answers & Explanations: **A, C, and D.** Answer **A** is incorrect, because Quick Mode and Main Mode are the two types of Security Associations that can be monitored in the Windows Firewall with Advanced Security. Answer **C** is incorrect, because Quick Mode and Main Mode are the two types of Security Associations that can be monitored in the Windows Firewall with Advanced Security. Answer **D** is incorrect, because Quick Mode and Main Mode are the two types of Security Associations that can be monitored in the Windows Firewall with Advanced Security.

10. What are the three firewall profiles you can use in the Windows Firewall with Advanced Security?
  - A. Public, Private, Network
  - B. Public, Home, Domain
  - C. Public, Private, Domain
  - D. Public, Work, Domain

Correct Answer & Explanation: **C.** The three firewall profiles you can use in the Windows Firewall with Advanced Security are Public, Private, and Domain

Incorrect Answers & Explanations: **A, B, and D.** Answer **A** is incorrect, because Network is not one of the profiles you can use in the Windows Firewall with Advanced Security. Answer **B** is incorrect, because Home is not one of the profiles you can use in the Windows Firewall with Advanced Security. Answer **D** is incorrect, because Work is not one of the profiles you can use in the Windows Firewall with Advanced Security.

## Chapter 5: 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 Answer & Explanation: **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 Answer & Explanation: **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 Answer & Explanation: **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 6: Application and Data Provisioning

1. What are the valid methods to contact Microsoft Licensing Clearinghouse to register and activate terminal server licenses?
  - A. Automatic Connection
  - B. E-mail
  - C. Web Browser
  - D. Telephone

Correct Answers & Explanation: **A, C, D.** When you need to register your terminal service licenses, the only three ways possible are via automatic connection, Web browser, and telephone. So answers **A, C, and D** are correct.

Incorrect Answer & Explanation: **B.** You cannot activate terminal licenses via e-mail—so answer **B** is wrong.

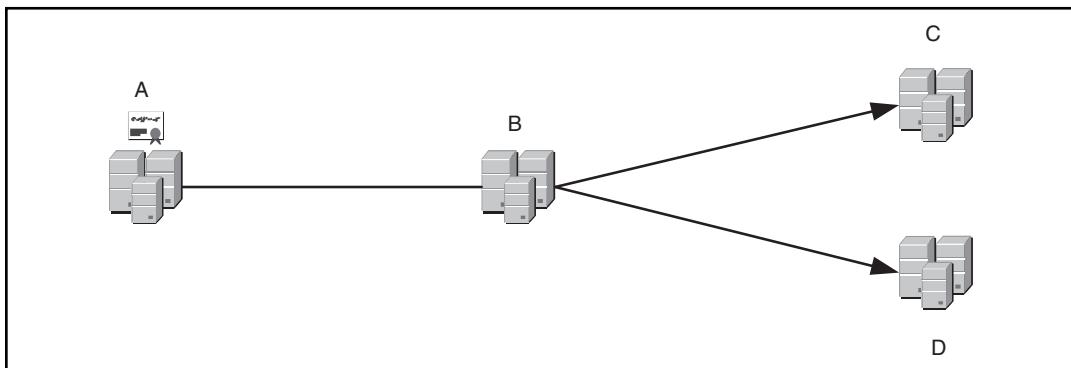
2. When planning a terminal server infrastructure, licensing choice, and design, Microsoft provides a couple of options concerning licensing types for terminal services. What are the licensing types available in Microsoft Windows 2008 Server?
- A. Per-Device Client Access License
  - B. Per-Server Client Access License
  - C. Per-User Client Access License
  - D. Per-Processor Access License

Correct Answers & Explanation: **A, C.** The only two license choices for Microsoft Windows 2008 Server Terminal Services are Per-Device and Per-User Client Access Licensing. This makes **A** and **C** correct.

Incorrect Answers & Explanation: **B, D.** Per-Server Client Access License is not an option in terminal server licensing—so answer **B** is incorrect. Per-Processor license is available for Microsoft SQL Server, but not for terminal services—so answer **D** is also incorrect.

3. In the following Visio drawing, Figure 6.44, which letter depicts the Windows 2008 Terminal Server License Server?
- A. A
  - B. B
  - C. C
  - D. D

**Figure 6.44** Terminal Server License Diagram



Correct Answer & Explanation: **B.** The correct answer would be answer **B** because it represents the Terminal License Server.

Incorrect Answers & Explanation: **A, C, D.** Answer **A** would represent the Microsoft Certificate Authority and License Clearinghouse—so answer **A** is wrong. Both servers **C** and **D** represent Microsoft Windows 2008 Terminal Servers—so answers **C** and **D** are incorrect.

4. You boss has asked you to install Terminal Services on a Microsoft Windows 2008 Server. What would be the first step in this process?

- A. Add the Terminal Server Role
- B. Add the Terminal Server Feature
- C. Add/Remove Programs
- D. Upgrade Microsoft Windows 2008 Server to Enterprise Edition

Correct Answer & Explanation: **A.** The correct answer to this question is **A**—you would need to add the Terminal Server Role.

Incorrect Answers & Explanation: **B, C, D.** You would only use Terminal Server Features to add specific items to Terminal Services—such as Licensing or TS Gateway. So answer **B** is incorrect. In Microsoft Windows 2008 Server—we no longer use the Add/Remove Programs control panel to add features to the operating systems. So answer **C** is incorrect. Terminal services will run on Microsoft Windows 2008 Server Standard Edition—so answer **D** is incorrect.

5. Microsoft Terminal Services Gateway Server allows us to connect to a Terminal Server securely from over the Internet with no other VPN technology. What are the protocols that are involved in this process?

- A. ICA
- B. RDP
- C. HTTPS
- D. HTTP

Correct Answers & Explanation: **B, C.** The correct answers are **B** and **C**—the HTTPS protocol encapsulates the RDP protocol allowing for a secured connection to the terminal server.

Incorrect & Explanation: **A, D.** The ICA protocol is a Citrix protocol—so answer **A** is incorrect. HTTP is not a secured protocol, so this would not be an option. Thus, answer **D** is incorrect.

6. Microsoft Terminal Services Gateway Server is dependent on other server roles and features that must be installed for Terminal Services Gateway Server to function properly. What are these other roles and/or features?
  - A. Remote Procedure Call (RDP) over HTTP Proxy
  - B. Application Server
  - C. Internet Information Services (IIS) 7.0
  - D. Network Policy and Access Services

Correct Answers & Explanation: **A, C, D.** The features and/or roles that need to be in place are Remote Procedure Call (RDP) over HTTP Proxy, Internet Information Services (IIS) 7.0, and Network Policy and Access Services—so answers **A, C**, and **D** are correct.

Incorrect Answer & Explanation: **B.** The Application Server role is not needed—so, answer **B** is incorrect.

7. When a client connects to a Terminal Server internally on a LAN with no encryption, what TCP port number is being used to establish this connection?
  - A. 443
  - B. 80
  - C. 3389
  - D. 1494

Correct Answer & Explanation: **C.** The client and server connection uses the RDP protocol that utilizes port 3389 TCP port to establish the connection—so answer **C** is correct.

Incorrect Answers & Explanation: **A, B, D.** Port 443 is the HTTPS protocol, so answer **A** is incorrect. Port 80 is the HTTP protocol making **B** also incorrect. The Citrix ICA protocol uses the 1494 TCP port—so answer **D** is also incorrect.

8. When you install Terminal Services Licensing, the server will issue temporary licenses during a “grace period.” How long do you have before this “grace period” expires?
  - A. 90 Days
  - B. 6 Months
  - C. 120 Days
  - D. 180 Days

Correct Answer & Explanation: **C.** When you install Microsoft Terminal Server Licensing, Microsoft gives you 120 days grace period to activate the licenses before they will stop working—so answer **C** is correct.

Incorrect Answers & Explanation: **A, B, D.** All other answers **A, B**, and **D** are incorrect.

9. In Microsoft Windows 2008 Server, Microsoft includes a Terminal Service feature called the Microsoft Terminal Services Session Broker (TS Session Broker). What are the two main functions of the TS Session Broker?
  - A. Enable a user to reconnect to an existing session.
  - B. Enable a user to connect over the Internet in a secured manner.
  - C. Enable session load-balancing.
  - D. Enable a user to connect to a Web site to start RDP connection.

Correct Answers & Explanation: **A, C.** The TS Session Broker is responsible for session load-balancing and reconnects users to disconnected sessions—thus, answers **A** and **C** are correct.

Incorrect Answers & Explanation: **B, D.** Terminal Server Gateway service allows for secured remote connections—so answer **B** is incorrect. Terminal Server Web Gateway is used to connect to RDP connections from a Web site—so answer **D** is incorrect.

10. You are an administrator of a midsized company. You would like to implement TS Session Broker service with two servers. One server is running Microsoft Windows 2008 Server Standard Edition and the other server is running Microsoft Windows 2003 Server Enterprise Edition. The clients are using an older copy of the Remote Desktop Connection (RDC) software. You have

worked on this installation for three days and still cannot get it to work. What is likely the problem or problems?

- A. You need to upgrade the Microsoft Windows 2008 Server Standard Edition to Enterprise Edition.
- B. The Remote Desktop Connection (RDC) software needs updated.
- C. Microsoft Windows 2003 Server needs to be upgraded to Microsoft Windows 2008 Server.
- D. The Microsoft Windows 2003 Server needs to have Service Pack 2 installed.

Correct Answers & Explanation: **B, C.** For TS Session Broker service to work, you must be using Remote Desktop Connection (RDC) software version 5.3 or later—so answer **B** is correct. Microsoft Windows 2003 Server cannot participate in a Microsoft Windows 2008 Server TS Session Broker installation—so answer **C** is correct.

Incorrect Answers & Explanation: **A, D.** TS Session Broker service is supported in all versions of Microsoft Windows 2008 Server, so answer **A** is incorrect. Installing Service Pack 2 on Microsoft Windows 2003 Server will not help the situation—Windows 2003 is not supported. Answer **D** is incorrect.

## Chapter 7: 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.

# Index

- 64-bit
  - adapters, 210
  - processors, 321–322
- 80/20 rule, 19
- 802.1x
  - IPSec study recommendation, 304
  - NAP enforcement, 28, 30
- A**
  - A (Host) record, 24
  - access
    - offline data, 449–451
    - Windows Server 2008 options for, 62
  - access permissions
    - access to users, groups, 63–64
    - allow/deny, 64
    - function of, 62
    - NTFS permissions, 65–68
    - Share Level permissions, File/Folder permissions, 62–63
  - Access Protection partners, 249
  - accounting, 253
  - acronyms, 226, 304
  - Active Directory (AD)
    - auditing, 296–298
    - deployment, planning for, 32–42
    - Directory Services backup, 523
    - domain for WDS, 43
    - Domain Services, 252
    - domains/forests, 76
    - GPOs, planning for, 125
    - objects, delegation of, 102–103
    - recovery by BitLocker Drive
      - Encryption, 474
    - replication of production database, 315, 316–317
  - SoftGrid Application Virtualization and, 373
- WSUS 3.0 SP1 settings to clients, 189, 191–196
- adapters, 210–211, 336–337
- Add Features* procedure, 484–486
- address assignment, DHCP, 12–13
- administration
  - application management, 103–107
  - delegating, 99–100, 149–150
  - delegating AD objects, 102–103
  - delegating authority, 100–102
  - remote, 85–87
- administration delegation
  - AD objects, 102–103
  - application management, 103–107
  - authority, 100–102
  - overview of, 99–100
  - agent-based backups, 521
  - Alias (CNAME) record, 24
  - allow* permission, 64
  - AMD-V processor, 322
- Application Development | .Net
  - Extensibility, 477
- application patching
  - description of, 196
  - third-party applications, 197
  - WSUS SP1, 197–199
- application services, 57–62
  - availability, 61–62
  - Hyper-V virtualization, 60–61
  - Web applications, 57–59
- applications
  - management strategy for, 103–107
  - management with SCVMM, 370–374
  - SCCM management/deployment of, 443–446
  - service redundancy at application level, 500
- virtualization of, 326–327, 424–425

- attacks. *See security*  
 auditing  
   AD/DS/LDS, 297–298  
   Event Log, 298–299  
   overview of, 295, 302  
   for virtual machine files, 540
- authentication  
   description of, 253  
   exemption rule, 282–283  
   IIS 7.0 methods, 58  
   method, IPSec, 274–279  
   source for SoftGrid Virtualization, 374
- authoritative restore, 525, 527
- authority, delegation of, 100–102
- authorization, 253
- automated server deployment, planning  
   for, 42–57  
   automation/scheduling, 54  
   Certificate Services, 54–57  
   standard server image, 53–54  
   Windows Deployment Services, 42–43  
   Windows Deployment Services,  
     installing/configuring, 43–53
- Automatic Updates, 189–196
- autonomous mode, WSUS server, 171
- availability  
   of ESX Server, 357  
   File and Print Server clustering, 71–73  
   Hyper-V installation and, 60, 61  
   *See also* High Availability
- B**
- backup and recovery  
   data recovery strategies, 520–521  
   DFSR for, 69  
   Directory Services, automated, 542  
   Directory Services, recovering,  
     523–527  
   dynamic backups, 464  
   full server backup with Windows Server  
     Backup, 510–519
- Geographically Disbursed Clustering  
   for, 542
- GPO, 140
- object level recovery with Windows  
   Server Backup, 527–534  
   overview of, 535, 539  
   server recovery, 521–523  
   of virtual machines, 315  
   Windows Server Backup design,  
     505–506  
   Windows Server Backup, installation of,  
     506–510
- Bare Metal Restore  
   of Directory Services, 524  
   methods for, 521–523
- baseline analysis  
   function of, 162  
   logging data collection in Reliability and  
     Performance Monitor, 221–222  
   performance measurement objects, 220
- BIOS, 322
- BitLocker  
   implementation of, 10–11  
   overview of, 292–294, 303  
   TPM and, 303
- BitLocker Drive Encryption  
   function of, 472–473  
   for hardware decommission,  
     420–421, 475  
   management options, 474–475  
   process of, 473–474  
   for protection of sensitive data, 540  
   volume recovery, 474
- BitLocker Remote Admin Tool, 475
- Block Inheritance, 138–140
- boundary network, 29
- bus, 209
- business continuity  
   backup and recovery, 505–534  
   data collaboration, 476–480  
   high availability, planning for, 481–505

methods/technologies for safeguarding resources, 464–465  
 overview of, 535–539  
 storage requirements, planning for, 465–475

## C

CA. *See* certification authority  
 cache, 209  
 CCR (Cluster Continuous Replication), 500  
 central processing unit (CPU), 213  
 Certificate Services  
     Certificate Servers, planning, 55–57  
     Public Key Infrastructure, 54–55  
 certification authority (CA)  
     authentication, 277, 278  
     planning, for server deployment, 55–57  
 child partition  
     of microkernel hypervisor, 320  
     parent partition and, 324  
     in virtualization architecture, 323  
 cipher command, 295  
 Cisco Network Access Control (NAC), 237  
 clients  
     NAP, 32, 250–251  
     RRAS, 243  
     for SCCM 2007 installation, 428, 434–436  
     WSUS 3.0 SP1 automatic updates, 189–196  
 cloning, 521  
 Cluster Continuous Replication (CCR), 500  
 clustering, 71–73  
     *See also* Failover Clustering  
 cmdlet, 91  
 CNAME (Alias) record, 24  
 collaboration. *See* data collaboration  
 command, cipher, 295  
 command line

Bare Metal Restore, 521, 523  
 BitLocker Drive Encryption installation via, 472  
 BitLocker Drive Encryption management with, 475  
 for Directory Services backup, 523  
 for Server Core installation, 355–356  
 Windows Firewall configuration with, 289–290  
 Windows PowerShell command-line interface, 364  
 Windows Server Backup installation via, 506, 507–508  
 Comments, Group Policy, 116–119  
 compatibility  
     Virtual Server 2005 R2 supported guest OSs, 328  
     virtualization for application compatibility, 326–327  
     of virtualized applications, 371, 372  
 computer  
     authentication of, 275–278  
     GPO configuration, 124–125  
 Computer Loopback policy, 151–152  
 Configuration API, 477, 478  
 connection  
     Remote Desktop, number allowed, 89 to WSUS, 188  
 connection security rules  
     authentication exemption, 282–283  
     creating, 279–280  
     isolation, 281–282  
     server-to-server, 284–285  
 Console Only installation, WSUS  
     installation of, 184–188  
     requirements for, 183  
 copper adapters, 210  
 corporate data center, 361–362  
 corruption, 466  
 CPU (central processing unit), 213  
 Critical Volume, 523, 524

**D**

data

- access, offline, 449–451
- accessibility, redundancy, 501–504
- collaboration, 476–480
- intellectual content, safeguarding, 464–465
- IPSec, modifying, 273–274
- recovery, 520–521
- redundancy, 464
- security, 471–475
- Self Healing NTFS, 466
- sensitive, protection of, 540

data collaboration

- overview of, 535, 536–537
- Windows Sharepoint Services for, 476–480, 541

Data Collector Sets, 203, 221–222

Data Execution Prevention (DEP), 322

data management

- definition of, 468
- Shared and Storage Management Console, 468–469
- Storage Explorer Console, 469–470
- Storage Manager for SANs Console, 470–471

data security

- BitLocker, 292–294
- encrypted file system, 294–295
- overview of, 291–292

Data Store, SoftGrid, 373

database, 173–174

DDNS (Dynamic DNS), 26

Delegate Authority, 100–101

delegation

- AD objects, 102–103
- administration, 99–100, 149–150
- authority, 100–102
- benefit of, 151
- deny* permission, 64
- DEP (Data Execution Prevention), 322

Detailed Replication, 296  
development testing environments, 314–317

device drivers

- microkernel hypervisor, 320–321
- monolithic hypervisor, 318–320
- VSP and, 324

DFS. *See* Distributed File System

DFSR (Distributed File System Replication), 69–70

DHCP. *See* Dynamic Host Configuration Protocol

digital locker, 303

Directory Services (DS)

- AD sites, site links, planning, 36–38
- auditing, 297–298
- automated backup, 542
- backup methods for, 523
- backup types for, 524
- description of, 32–33
- domain controller placement, 35
- forests/domains, 33–35
- OU, delegating permissions to, 40–42
- OU design, 38–39
- recovery of, 523–527
- replication, 296
- Restore Mode, 524–525
- RODCs, planning for, 36

disaster recovery

- for data assets protection, 464–465
  - DFSR for, 69
  - Geographically Disbursed Clustering for, 542
  - heartbeat delay and, 499
  - virtualization technology for, 317–318
- See also* backup and recovery

Distributed File System (DFS)

- for data accessibility, redundancy, 503–504
- installing, 448–449
- overview of, 447–448, 453
- for service availability, 501

Distributed File System Replication (DFSR), 69–70

Distributed Transaction Coordinator Service, 501

distribution package, 444–446

DNS. *See* Domain Name System

domain controller, 35–37

Domain Name System (DNS)

- AD deployment of, 21–22
- function of, 20
- name resolution process, 20–21
- records, 24–27
- Round Robin DNS, 58
- for WDS, 43
- zones, 22–24

domains

- deployment, planning for, 33–34
- domains/forests for typical deployment, 76
- in GPO hierarchy, 126–128

downstream server, 170–171

DRA (dynamic resource allocation), 357

DS. *See* Directory Services

dynamic backup, 464

Dynamic DNS (DDNS), 26

Dynamic Host Configuration Protocol (DHCP)

- address assignment, 12–13
- DHCP NAP enforcement, planning for, 28, 29
- infrastructure services, planning, 11–12
- installation/configuration of, 13–19
- NAP and, 251
- for service availability, 501
- for WDS, 43

Dynamic Least Queue Depth, 468

dynamic resource allocation (DRA), 357

**E**

efficiency, 311

emulation, 328

encryption

- BitLocker, implementation of, 10–11
- BitLocker Drive Encryption, 472–475, 540
- encrypted file system, 294–295
- PKI, 54–57

End User License Agreement (EULA), 346

Enforce, 134–138

enforcement methods, NAP, 27–31

enforcement points, NAP, 251–252

Enterprise Certificate Authority (CA), 55

enterprise environment, 361–362

equal\_per\_session policy, 421–424

ESX Server, VMware, 356–358

Event Log, 298–299

event management, 217–219

Event Subscriptions, 299

Event Viewer, 218–219

exceptions, firewall

- built-in, 261–263
- manual, 263–266

Exchange Service, 500

export, 289, 303

**F**

failback, 467

Failover Clustering

- architecture of, 482–483
- for availability, 61
- data accessibility, redundancy, 501–503
- Geographically Disbursed Clustering, 542
- for high availability, 481
- Hyper-V virtualization and, 504–505, 541
- installation of, 484–498
- multi-site clusters, 498–499
- new features of, 481–482
- NLB *vs.*, 76
- service availability, 501
- service redundancy, 499–500

Failover Clustering File Services, 503

Failover Clustering Management  
     Console, 502  
 failover redundancy, 467–468  
 failover-based load balancing, 467  
 Feature Delegation, 58  
 fiber adapters, 210  
 File and Print server clustering, 71–73  
 File and Print services, 62–73  
     access permissions, 62–68  
     availability options, 71–73  
     indexing files, 70  
     printers, publishing, 73  
     replication with DFSR, 69–70  
     storage policies, 70–71  
         Storage Quotas, 69  
 file screens, 70–71  
 File Server Role, 502  
 file services cluster, 502–503  
 file system, encrypted, 294–295  
 File Transfer Protocol (FTP), 59  
 File/Folder permissions, 62–63  
 files  
     DFSR for distribution of, 69  
     recovery with Windows Server Backup, 527–534  
         Self Healing NTFS, 466  
         virtual machine files, security of, 540–541  
 firewall. *See* Windows Firewall  
 firewall rules  
     creating, 285–286  
     inbound rules, 287–288  
 Folder, DFS, 447–448  
 forests  
     deployment, planning for, 33–35  
     domains/forests for typical  
         deployment, 76  
     function of, 34  
 forward lookup query, 20–21  
 forwarding, DNS, 26–27  
 FTP (File Transfer Protocol), 59  
 full backup, 510–519, 524

## G

GeoCluster, 71–73  
 Geographically Disbursed Clustering, 542  
 Global Naming Zones (GNZ), 23–24  
 GPT (Group Policy Template), 113  
 Granular Audit Policy (GAP), 299  
 Group Policy  
     computer configuration, 124–125  
     description of, 151  
     GPOs, non-local, 113–123  
     GPOs, planning for, 125–130  
     local, 110–113  
     recovery by BitLocker Drive  
         Encryption, 474  
     removable media control, 471–472, 540  
     strategy, planning overview, 107–109  
     Targeting *vs.*, 122  
     types of, 109–110  
     user configuration, 123–124  
     Windows 2008 features, 152  
 Group Policy Container, 113  
 Group Policy, controlling application of  
     Block Inheritance, 138–140  
     Enforce, 134–138  
     GPO backup/recovery, 140  
     overview of, 134, 150  
     troubleshooting, 140–147  
 Group Policy Modeling, 141, 144–147  
 Group Policy Object (GPO)  
     backup/recovery of, 140  
     BitLocker Drive Encryption and, 474  
     creating/linking, 130–131, 150  
     creating/linking at one time, 133–134  
     existing, linking, 131–132  
     planning for, 125–126  
     processing priority, 128–130  
     site/domain/OU hierarchy, 126–128  
     stand-alone, creating, 131  
     for WSUS 3.0 SP1 settings to clients, 189, 191–196  
 Group Policy Results, 141–144

Group Policy Template (GPT), 113  
 groups  
   access permissions for, 63–64  
   permission delegation, 100  
 guest operating system  
   categories of, 325–326  
   monolithic hypervisor’s support of, 319  
   supported options for, 345  
   Virtual Server 2005 R2 support of, 328  
   in virtualization architecture, 322–323  
   VSP and, 324  
 guest with enlightened operating system,  
   325–326  
 guest with partially enlightened operating  
   system, 326

**H**

hands-on training, 163, 226  
 hardware  
   BitLocker Drive Encryption for  
     decommissioning, 475  
   inventory, 436–439  
   load balancing for Web applications, 57  
   redundancy, 464, 467–468  
   requirements for Windows Server 2008,  
     2–3  
   hardware assisted virtualization, 329, 356  
   hardware requirements  
     hardware RAID levels, 211–212  
     for Hyper-V, 60  
     server, 209  
     server network, storage adapter, 210–211  
   HCAP (Host Credential Authorization  
     Protocol), 236  
   health certificate, 29  
   Health Policy Server, 31, 252–253  
   Health Registration Authority (HRA),  
     31, 236, 251  
   Health Requirement Server, 31, 254  
   heartbeat, 498, 499  
   hierarchy, policy, 138

High Availability  
   data accessibility, redundancy, 501–504  
   Failover Clustering, 481–499  
   Hyper-V virtualization and, 504–505  
   overview of, 535, 537–538  
   service availability, 501  
   service redundancy, 499–500  
   solutions for, 481  
 High Availability Wizard, 501  
 historical monitoring, 202  
 Host (A) record, 24  
 Host Credential Authorization Protocol  
   (HCAP), 236  
 HRA. *See* Health Registration Authority  
 Hyper-V  
   architecture of, 321–326  
   competition comparison, 356–358  
   with Failover Clustering, 541  
   high availability and, 504–505  
   installation, configuration of, 61–62  
   introduction of, 57  
   planning for deployment of, 60–61  
   RCO update for Virtualization Role,  
     331–332  
   SCVMM and, 364  
   Virtual Server 2005 R2 SP1 *vs.*, 330–331  
   virtual server configuration with,  
     344–354  
   Windows Server Virtualization Role,  
     installation of, 332–344

hypervisor  
   microkernel, 320–321  
   monolithic, 318–320

**I**

IIS. *See* Internet Information Services (IIS)  
   6.0; Internet Information Services  
     (IIS) 7.0  
   images, 50–52, 54  
   import, 289, 303  
   inbound rules, 287–288

- index file, 70
- infrastructure services, planning for, 11–42  
  address assignment, 12–13  
  DHCP, installing/configuring, 13–19  
  directory services, 32–42  
  Domain Name System, 20–27  
  importance of, 11–12  
  Network Access Protection, 27–32
- inheritance, policy, 128, 138–140
- Initial Configuration Tasks Window, 506
- installation  
  of Windows Server 2008, 5–10  
  of WSUS Server 3.0 SP1, 172–183  
  of WSV Role, 332–344
- installation or upgrade, planning for  
  BitLocker, implementation of, 10–11  
  choice between installation/upgrade, 2  
  installing Windows Server 2008, 5–10  
  rollback planning, 5  
  virtualization licensing, 4  
  Windows Server 2008 edition, selection  
    of, 3–4
- Intel VT processor, 322
- intellectual content  
  data collaboration with WSS, 476–480  
  safeguarding, 464–465  
  *See also* business continuity
- intermediate CA, 56–57
- Internet Authentication Service, 303
- Internet Information Services (IIS) 6.0, 477
- Internet Information Services (IIS) 7.0  
  authentication methods, 58  
  delegation, remote administration, 58–59  
  deployment planning, 57  
  FTP, POP3, SMTP services, 59  
  for WSUS 3.0 SP1, 166–169
- Internet Protocol Security (IPSec)  
  IPSec NAP enforcement, planning for, 28, 29  
  L2TP and, 247  
  Internet Protocol Security (IPSec) defaults
- authentication method, 274–279  
  data protection, 273–274  
  key exchange, 272–273  
  overview of, 270–272
- interrupt moderation, 211
- inter-site replication, 37
- intra-site replication, 37
- IP address  
  DHCP assignment of, 12–13  
  DHCP installation/configuration, 13–19  
  DNS name resolution for, 20–21  
  Network Access Protection, 27–32
- IP Security enforcement, 304
- IPSec. *See* Internet Protocol Security
- isolation, 281–282, 310
- ## K
- Kerberos V5, 277, 278
- Kernel Mode process level, 324, 325
- key exchange, 272–273
- keys, 54–57, 278, 475
- Knowledge Consistency Checker  
  (KCC), 37
- ## L
- laboratory environments, 314–317
- languages, 171, 179–180
- Layer 2 Tunneling Protocol (L2TP), 247
- LDS (Lightweight Directory Services), 297–298
- learning curve, 313
- legacy guest, 326
- legacy operating system, 381
- LGPOs (Local Group Policy Objects), 110
- library, Virtual Machine Manager Library, 365–366
- licensing  
  Terminal Services, 391–392, 452  
  virtualization, 4
- Lightweight Directory Services (LDS), 297–298

linking  
 GPOs, existing, 131–132  
 GPOs, when creating, 133–134, 150

load balancing  
 Multipath I/O for, 467–468  
 virtual server placement and, 359  
 for Web farms, 57–58  
*See also* Network Load Balancing

Local Group Policy Objects (LGPOs), 110

log files, 270

logging, 220, 221–222

lookup query, 20–21

## M

Mail Exchanger (MX) record, 24–25

main mode, 272–273

Majority Quorum Model, 483

malicious code, 322

management  
 of applications with SCVMM, 370–374  
 BitLocker Drive Encryption, 474–475  
 data management, 468–471  
 with Hyper-V, 60  
 interface, common, 311  
 server virtualization and, 312  
 servers in Windows Server Virtualization, 368–369

Management Console, SoftGrid, 373

management strategy, server  
 overview of, 84–85  
 remote administration, 85–87  
 Remote Desktop, 87–91

Server Management Technologies, 91–93

Server Manager, 93–99

MAP (Microsoft Assessment and Planning), 3

memory  
 server hardware recommendations, 209

Virtual Server 2005 R2 SP1 support of, 329

memory stick, 471–472

microkernel hypervisor, 320–322

Microsoft Assessment and Planning (MAP), 3

Microsoft Licensing Clearinghouse, 452

Microsoft Management Console (MMC), 183–188

Microsoft Office Sharepoint Services 2003, 476

Microsoft SoftGrid Application Virtualization, 370–374, 425

Microsoft SQL Server, 428

Microsoft System Centers Essentials 2007 features of, 163–164  
 for third-party application patching, 196, 197

Microsoft Terminal Services Client (MSTSC), 90–91

Microsoft Terminal Services Gateway, 404–408

Microsoft Virtual PC 2007, 390

Microsoft Virtualization  
 description of, 452  
 overview of, 424–426, 454

Microsoft Windows 2008 Server Terminal License Server, 392–397

Microsoft Windows 2008 Server Terminal Server, 397–402

Microsoft Windows Mobile, 249

Microsoft Windows Server 2008. *See* Windows Server 2008

Microsoft Word Viewer, 444–446

migration  
 strategy for P2V conversion, 383  
 System Center Virtual Machine Manager and, 366–367

VMware, management of, 374–375

MMC (Microsoft Management Console), 183–188

monitoring, 162  
*See also* patch management; performance monitoring

monolithic hypervisor, 318–320  
 MSTSC (Microsoft Terminal Services Client), 90–91  
 Multipath I/O (MPIO), 467–468  
 Multiple Local Group Policy Objects (MLGPOs), 110, 111–113  
 multi-site clusters, 498–499  
 MX (Mail Exchanger) record, 24–25

**N**

NAC (Network Access Control), 237  
 name resolution, 20–27  
 Name Server (NS) record, 25  
 Name Servers (NS). *See* Domain Name System (DNS)  
 Namespace Root, 447–448  
 Namespace Server, 447–448  
 NAP. *See* Network Access Protection  
 .NET Framework 3.0, 477–478  
 NETBIOS, 23–24  
 Network Access Control (NAC), 237  
 Network Access Protection (NAP)  
     802.1x NAP enforcement, 30  
     AD Domain Services, 252  
     clients, 250–251  
     clients, planning for, 32  
     DHCP NAP enforcement, 29  
     enforcement methods, planning for, 27–28  
     enforcement points, 251–252  
     Health Policy Server, 252–253  
     Health Requirement Server, 254  
     IPSec NAP enforcement, 29  
     network layer protection, 249–250  
     overview of, 248–249  
     partners, 249  
     restricted network, 254–255  
     server deployment, planning for, 31–32  
     software policy validation, 255–256  
     VPN NAP enforcement, 30–31

Network Access Quarantine Control, 248, 303  
 network adapters, 210–211, 336–337  
 Network Interface Cards (NICs), 242–243  
 network interfaces, NPAS, 242–243  
 network layer protection, 249–250  
 Network Load Balancing (NLB)  
     for availability, 61  
     Failover Clustering *vs.*, 76  
     for high availability, 481  
     for Web applications, 57–58  
 Network Location Awareness, 122–123  
 Network Policies and Access (NPAS)  
     description of, 300  
     installing with RRAS, 238–242  
     role, installing/configuring, 237  
 networks, restricted, 254–255  
 NICs (Network Interface Cards), 242–243  
 NLB. *See* Network Load Balancing  
 non-authoritative restore, 525–526  
 Non-Local Group Policy Objects (GPOs), 113–123  
 NPAS. *See* Network Policies and Access  
 NS (Name Server) record, 25  
 NTFS, Self Healing, 466  
 NTFS permissions  
     allow/deny, 64  
     configuration of, 65–68  
     Share permissions *vs.*, 62–63  
 NTLMv2, 277, 278

**O**

object level recovery, 527–534  
 Office Communicator Remote Access, 236  
 offline files, 449–451  
 offload capability, 211  
 operating system (OS)  
     guest, categories of, 325–326  
     guest, in virtualization architecture, 322–323

- guest, monolithic hypervisor's support of, 319
- legacy, SoftGrid Application Virtualization and, 381
- OS level patch management, 164–188
- SCCM deployment of, 446–447
- for Virtual Server 2005 R2, 327–329
- virtualized application and, 370, 371
- WinRE Bare Metal Restore, 522
- WSUS 3.0 SP1 automatic updates and, 189
- for WSUS 3.0 SP1 Console Only installation, 183
- optimization
- server hardware design, 208–213
  - of servers, 162, 226–227
  - tuning, 208
- WSRM/Process Matching Criteria, 214–218
- Organizational Unit (OU)
- design, planning, 38–39
  - function of, 34
  - in GPO hierarchy, 126–128
  - permissions, delegating to, 40–42
- OS. *See* operating system
- Outlook Anywhere, 235
- P**
- P2V (physical-to-virtual) migration, 366–367, 383
- package, distribution, 444–446
- parent partition, 320, 323–324
- partitions, 320, 323–324
- patch management
- application patching, 196–199
  - Microsoft Systems Centers Essentials 2007, 163–164
  - overview of, 223–225
  - Windows Server Update Service for, 162–163
  - Windows Update, enabling, 164–166
- WSUS, installation of IIS 7.0 components for, 166–169
- WSUS, secure connection to, 188
- WSUS 3.0 SP1, automatic updates for clients, 189–196
- WSUS 3.0 SP1 deployment, 169–171
- WSUS 3.0 SP1 installation, 172–183
- WSUS 3.0 SP1 MMC, 183–188
- performance
- BitLocker Drive Encryption and, 473
  - microkernel hypervisor and, 321
  - monolithic hypervisor and, 318, 319
  - virtual machine placement and, 359
- Performance and Reliability Monitor, 203, 206–208
- performance counters, 206–208
- Performance Monitor tool, 92
- performance monitoring
- event/service management, 217–219
  - importance of, 199–200
  - monitoring servers, 202–206
  - optimization, 208–217
  - overview of, 224, 225
  - questions on exam regarding, 226
- Reliability and Performance Monitor, opening, 200–202
- system activity monitoring, 206–208
- trending, baseline analysis, 220–222
- permissions
- access permissions, 62–65
  - application of, 76
  - NTFS, 65–68
  - OU, delegation of, 40–42
  - OU design and, 38–39
- physical-to-virtual (P2V) migration, 366–367, 383
- PKI (Public Key Infrastructure), 54–57
- placement, of virtual servers, 358–360, 382
- planning, for server deployment
- application services, 57–62
  - automated server deployment, 42–57

- planning, for server deployment (*Continued*)  
     file and print services, 62–73  
     infrastructure services, 11–42  
     installation or upgrade, 2–11  
     overview of, 74–75
- Pointer (PTR) record, 25
- Point-to-Point Tunneling Protocol (PPTP),  
     244–247
- ports  
     firewall exceptions, 263  
     L2TP/IPSec, 247  
     PPTP, 244–247  
     RRAS, 244  
     SSTP, 247–248
- Post Office Protocol (POP3), 59
- PowerShell  
     command-line interface, 364  
     description of, 91–92, 151  
     for Directory Services backup, 542  
     for P2V process, 367  
     server management with, 368  
     VMware, management of, 374–375
- PPTP (Point-to-Point Tunneling Protocol),  
     244–247
- PreBoot Execution Environment (PXE)  
     description of, 92  
     server for WDS, 43  
     Virtual Server 2005 R2 support of, 329  
     in WDS configuration, 49–50
- Preferences, Group Policy, 119–122
- preshared key, 278
- primary zone, 23
- Print services, 501  
     *See also* File and Print services
- printers, publishing, 73
- priority, processing, 128–130
- private key, 54–55
- Process Model, for Windows Sharepoint  
     Services, 477, 478
- processing priority, Group Policy, 128–130
- processors  
     for Hyper-V virtualization, 321–322  
     server hardware recommendations, 209
- provisioning, application  
     application virtualization, 424–425  
     overview of, 390–391, 454  
     resource allocation, 419–424  
     Terminal Server infrastructure, 391–419
- provisioning, data  
     offline data access, 449–450  
     offline files, working with, 450–451  
     overview of, 390, 447, 455  
     Server Distributed File System, installing,  
         448–449  
     shared resources, working with, 447–448
- PTR (Pointer) record, 25
- public key, 54–55
- Public Key Infrastructure (PKI), 54–57
- PXE. *See* Pre-Boot Execution  
     Environment
- Q**
- quality assurance, 314–315
- quick mode, 273–274
- Quorum, 482–483
- R**
- RADIUS (Remote Authentication Dial-In  
     User Service), 236
- RAID, 211–213, 227
- RAID 0, 212
- RAID 0+1, 212–213
- RAID 1, 212–213
- RAID 5, 212
- RAID 6, 212
- Read-Only Domain Controllers  
     (RODCs), 36
- real time monitoring, 202
- records, DNS  
     DDNS, planning for, 26  
     DNS forwarding, planning for, 26–27  
     list of common, 24–25

- recovery
  - GPO, 140
  - password for BitLocker Drive
    - Encryption, 474
  - virtualization technology for, 317–318
- See also* backup and recovery; disaster recovery
- redundancy
  - data, solutions for, 501–504
  - for data assets protection, 464–465
  - DNS deployment plan for, 21
  - File and Print server clustering, 71–73
  - for high availability, 481
  - Multipath I/O for, 467–468
  - service redundancy features, 499–500
- registry file, 189–191
- Reliability and Performance Monitor
  - description of, 92–93
  - logging data collection in, 221–222
  - monitoring system activity with, 206–208
  - new features of, 203
  - opening, 200–202
  - overview of, 92–93
  - Resource View details, 203–205
- remediation VLAN, 30
- remote access security
  - NAP, 248–256
  - NPAS, installing/configuring, 237
  - overview of, 235–237, 300, 301
  - RRAS, 237–247
- remote administration
  - description of, 59
  - management strategy for, 85–87
  - tools for, 151
- Remote Authentication Dial-In User Service (RADIUS), 236
- Remote Desktop
  - description of, 151
  - management strategy for, 87–91
- Remote Desktop Protocol (RDP)
  - for application management, 104–105
  - description of, 87
- Remote Server, 355
- RemoteApp
  - for application management, 104–105
  - description of, 152
- removable media, 471–472, 540
- replica mode, 171
- replication
  - AD replication topology, 37–38
  - planning for, 69–70
  - Standby Continuous Replication, 500
- resilience, 61
- resource allocation
  - overview of, 419, 452
  - System Resource Manager, 420–424
- Resource Overview, of Reliability and Performance Monitor, 203–205
- resources
  - intellectual content, safeguarding, 464–465
  - Server Core installation and, 354
  - server resource usage and
    - virtualization, 60
  - server virtualization benefit, 312
  - shared, 447–448
  - for virtual machine, 346
  - virtual machine placement and, 359
  - virtualization parent partition and, 323–324
- See also* business continuity
- response time, 312
- restore. *See* backup and recovery; disaster recovery; recovery
- restricted network, 29, 254–255
- reverse DNS zones, 23
- RODCs (Read-Only Domain Controllers), 36
- roles
  - DFS, 453
  - in DHCP installation, 13–15

- roles (*Continued*)
  - NPAS, 237–242, 300
  - RRAS, 237–238
  - server, adding, 95–98
  - WSv Role installation, 332
  - See also* Server roles
- rollback, 5
- root CA, 56–57
- root hints, 27
- Round Robin
  - DNS for Web applications, 58
  - Multipath I/O configuration, 467, 468
- Routing and Remote Access Service (RRAS)
  - clients, 243
  - network interfaces, 242–243
  - NPAS role, installing with, 238–242
  - overview of, 237–238
  - ports, 244–247
- rules
  - authentication exemption, 282–283
  - connection security, 279–281
  - firewall, 285–286
  - inbound, 287–288
  - isolation, 281–282
  - server-to-server connection security, 284–285
- S**
  - SACL (System Access Control List), 297
  - SANs (Storage Area Networks), 470–471
  - scavenging, 26
  - SCC (Single Copy Clusters), 500
  - SCCM. *See* System Center Configuration Manager 2007
    - scheduling, image deployment, 54
    - scope, 18
  - SCR (Standby Continuous Replication), 500
  - search, 70
  - secondary zone, 23
- secure network, 29
- Secure Online Key Backup, 303
- Secure Socket Layer (SSL), 188
- Secure Socket Tunneling Protocol (SSTP), 247–248, 303
- security
  - BitLocker, implementation of, 10–11
  - Certificate Services, 54–57
  - data security features, 471–475
  - of Failover Clustering, 482
  - microkernel hypervisor and, 321
  - monolithic hypervisor and, 319–320
  - overview of, 234–235
  - Server Core installation and, 354
  - virtualization parent partition and, 323
  - virtualization technology and, 316
  - See also* auditing; patch management; remote access security
- security, server
  - connection security rules, 279–285
  - data security, 291–295
  - firewall rules, 285–290
  - IPSec defaults, 270–279
  - overview of, 256, 301
  - Windows Firewall, advanced configuration of, 267–270
  - Windows Firewall management, 257–266
  - Windows Firewall, monitoring, 290–291
- Security Templates, 149
- Self Healing NTFS, 466
- Self Service Web Portal, System Center
  - Virtual Machine Manager, 364–365
- sequencing, application, 373
- server consolidation
  - benefits of, 310, 313–314
  - plan for, 381
- Server Core installation
  - data recovery and, 520
  - for Hyper-V virtualization platform, 354–356
  - Windows Sharepoint Services on, 476

server deployment, planning for application services, 57–62  
 automated server deployment, 42–57  
 file and print services, 62–73  
 infrastructure services, 11–42  
 installation or upgrade, 2–11  
 overview of, 74–75  
 server hierarchy, 170–171  
 server image  
     automation, scheduling, 54  
     deployment planning, 53–54  
     in WDS configuration, 50–52  
 server management, planning for administration delegation, 99–107  
 GPOs, creating/linking, 130–134  
 group policies, controlling application of, 134–147  
 Group Policy strategy, planning, 107–130  
 overview of, 84, 148  
 strategy, 84–99  
**Server Management Technologies**  
 Windows Deployment Services, 92  
 Windows PowerShell, 91–92  
 Windows Reliability and Performance Monitor, 92–93  
**Server Manager**  
 BitLocker Drive Encryption installation via, 472  
 description of, 151  
 management strategy for, 93–98  
 Server Core installation remote management with, 355  
 ServerManagerCMD, 98–99  
 virtual machine creation with, 344–345  
 Windows Server Backup installation via, 506  
 Windows Virtualization Manager from, 343  
 WSv Role installation from, 332–344

**Server Roles**  
 Windows Server Virtualization Role, installation of, 332–344  
 Windows Sharepoint Services Role, 476–478, 479  
 server security. *See* security, server  
 server virtualization  
     application compatibility, 326–327  
     architecture, 321–326  
     benefits of, 311–312  
     data recovery and, 520–521  
     description of, 310–311  
     disaster recovery, 317–318  
     Hyper-V, 330–331  
     Hyper-V, installation/configuration, 61–62  
     Hyper-V RCO update for configuration, 331–332  
     implementation issues, 312–313  
     importance of, 310  
     microkernel hypervisor, 320–321  
     monolithic hypervisor, 318–320  
     overview of, 376–377  
     planning for, 60–61  
     quality assurance, development testing environments, 314–315  
 server consolidation, 313–314  
 Server Core, 354–356  
 server placement, 358–360  
 System Center Virtual Machine Manager 2007, 360–375  
 threats to security/stability, 316–317  
 Virtual Server 2005, 327–330  
 virtual server configuration with Hyper-V, 344–354  
 Windows Server Virtualization, competition comparison, 356–358  
 Windows Server Virtualization, installation of, 332–344  
 ServerManagerCMD, 98–99

- servers
  - Bare Metal Restore, 521–523
  - hardware design, 208–213
  - monitoring, 202–206
  - NAP, planning for, 31–32
  - optimization of, 208–217
  - trending, baseline analysis, 162
  - Windows Server Virtualization management, 368–369
- See also* patch management; virtual servers
- server-to-server connection security rule, 284–285
- Service (SRV) record, 25
- service availability, 501
- service management, 217
- service redundancy, 499–500
- Share level permissions
  - allow/deny, 64
  - assignment of, 76
  - File/Folder permissions *vs.*, 62–63
- shared resources, 447–448
- SHVs (System Health Validators), 255–256
- Simple Mail Transfer Protocol (SMTP), 59
- Single Copy Clusters (SCC), 500
- site links, AD, 36–38
- sites
  - description of, 109
  - in GPO hierarchy, 126–128
- sites, AD
  - definition of, 34
  - planning, 36–38
- SMS (Systems Management Server), 426
- SMTP (Simple Mail Transfer Protocol), 59
- snapshots, 521, 528
- SoftGrid Application Virtualization
  - application management with, 370–374
  - candidate for, 381
  - overview of, 425
- SoftGrid Desktop Client, 374
- SoftGrid Sequencer, 373
- SoftGrid Terminal Services Client, 374
- Softricity, 370
- software
  - inventory, 439–443
  - policy validation, NAP and, 255–256
  - WSUS 3.0 SP1 requirements, 169–170, 183
- Software Inventory Client Agent, 440–443
- SQL Server 2005, 360–361
- SRV (Service) record, 25
- SSL (Secure Socket Layer), 188
- SSTP (Secure Socket Tunneling Protocol), 247–248, 303
- stability, 317, 319–320, 482
- Stand-Alone Certificate Authority (CA), 55
- stand-alone GPOs, 128–130, 131
- stand-alone instance, 361
- Stand-Alone Virtualization Management
  - Console
  - choice of, 343–344
  - server management with, 368
  - virtual machine creation with, 344–345, 346–354
- standards, for server virtualization, 313
- Standby Continuous Replication (SCR), 500
- StarterGPOs, 149, 152
- storage
  - for Failover Clustering, 502
  - file screens, 70–71
  - quotas, 69
  - server hardware, performance and, 211–213
  - Virtual Machine Manager Library, 365–366
  - for WSUS 3.0 SP1, 170
- storage adapters, 210–211
- Storage Area Networks (SANs), 470–471
- storage requirements
  - data management, 468–471
  - data security, 471–475

- Multipath I/O, 467–468  
 overview of, 535–536  
 Self Healing NTFS, 466  
 Windows 2008 Server improvements, 465  
 strategy  
   Group Policy, planning, 107–109, 150  
   management, developing, 84–85, 149  
 stub zone, 23  
 subnet, 499  
 subordinate CA, 56–57  
 subscriptions, 299  
 System Access Control List (SACL), 297  
 system activity monitoring, 206–208  
 System Center Configuration  
   Manager 2007  
     application management/deployment, 443–446  
     client, installing, 434–435  
     description of, 390  
     hardware inventory, 436–439  
     Management Console, installing on Vista, 429–434  
     OS deployment, 446–447  
     overview of, 390, 426–429, 453, 454  
     software inventory, 439–443  
     for third-party application patching, 197  
 System Center Operations Manager  
   integration/compatibility of, 357  
   migration support, 366  
   SCVMM and, 361  
   server placement and, 360, 382  
 System Center Virtual Application  
   Server, 373  
 System Center Virtual Machine  
   Manager 2007  
     applications, managing, 370–374  
     integration/compatibility of, 357  
     migration support functionality, 366–367  
     overview of, 360–362, 379  
     Self Service Web Portal, 364–365  
     server management with, 368  
   servers, managing, 368–369  
 Stand-Alone Virtualization Management  
   Console, 369  
   virtual assets management, 381–383  
   virtual machine creation with, 344–345, 367  
 Virtual Machine Manager Administrator  
   Console, 362–364  
 Virtual Machine Manager Library, 365–366  
 virtual server placement, 359–360  
 VMware, managing, 374–375  
 Windows PowerShell command-line  
   interface, 364  
 System Center Virtual Machine Manager  
   Administrator Console, 362–364  
 System Center Virtual Machine Manager  
   Self Service Web Portal, 364–365  
 System Health Validators (SHVs), 255–256  
 System Resource Manager, 420–424  
 Systems Management Server (SMS), 426

**T**

- Targeting, 121  
 templates, 149, 203  
 Terminal License Server, 392–397  
 Terminal Server  
   installing, 397–402  
   overview of, 452  
 Terminal Server infrastructure  
   2008 Server TS License Server, installing, 392–397  
   2008 Server TS Server, installing, 397–402  
   Terminal Services Gateway Server, 402–419  
   TS licensing, 391–392  
 Terminal Services  
   for application management, 100  
   exam recommendations for, 456–457  
   Server Core installation remote  
     management with, 355

- Terminal Services (*Continued*)  
     virtualized application compatibility  
         with, 371
- Terminal Services Gateway Server  
     NAP enforcement, 28  
     overview of, 402–403  
     TS Gateway, installing, 404–408
- Terminal Services RemoteApp  
     description of, 236  
     installing from Windows Installer Package,  
         414–419  
     overview of, 413, 452
- Terminal Services Session Broker  
     installing, 410–412  
     overview of, 409–410, 452
- Terminal Services Web Access (TSWA),  
     106–107, 152
- third-party applications, 196–197
- threats, 316–317  
     *See also* security
- thumbnail Console window, 364
- training, hands-on, 163
- trees, 33
- trending, 220–222
- troubleshooting, GPO, 140–147
- Trusted Platform Module (TPM)  
     BitLocker and, 292–294, 303  
     for encryption of files, 473–474
- U**
- updates, 331–332  
     *See also* patch management
- upgrade  
     choice between installation/upgrade, 2–3  
     rollback planning, 5  
     virtualization licensing, 4  
     from Windows Server 2003 to 2008, 76  
     Windows Server 2008 edition, selection  
         of, 3–4
- upstream server, 170–171, 177–179
- User Mode process level, 324, 325
- users  
     access permissions for, 63–64  
     authentication, 278–279  
     GPO configuration, 123–124  
     permission delegation, 100
- V**
- V2V (virtual-to-virtual) conversion, 367,  
     374–375
- .vhdx file format  
     placement of, 358  
     security risk of, 316  
     .vmdk file migration to, 361, 374–375  
     VSS backup to, 506
- virtual assets, 312
- virtual capacity, 311
- Virtual Local Area Networks (VLANs),  
     255, 304
- Virtual Machine Manager Library,  
     365–366
- Virtual Machine Service (VMS), 324
- Virtual Machine Worker Processes, 324
- virtual machines  
     configuration of with Hyper-V, 344–354  
     creation process with SCVMM, 367  
     file security, 540–541  
     high availability with Hyper-V, 504–505  
     server placement, 358–360  
     System Center Virtual Machine Manager  
         2007, 360–375
- Virtual Private Network (VPN), 28, 30–31
- Virtual Server 2005 Enterprise Edition, 328
- Virtual Server 2005 R2  
     functionality upgrades, 329–330  
     guest operating systems supported by,  
         328–329  
     operating system for host support of,  
         327–328  
     PXE boot support, 329
- Virtual Server 2005 R2 SP1  
     for 64-bit host OS, 327

- functionality upgrades, 329  
 Hyper-V *vs.*, 330–331  
 Virtual Server 2005 Standard Edition, 328  
 virtual servers  
   configuration of with Hyper-V, 344–354  
   data recovery and, 520–521  
   placement of, 358–360, 382  
   SCVMM migration support, 366–367  
 virtualization  
   application, 326–327, 424–425  
   data recovery and, 520–521  
   Failover Clustering and, 541  
   high availability and, 504–505  
   Hyper-V, 57  
   Hyper-V, installation/configuration, 61–62  
   licensing, 4  
   planning for, 60–61  
   *See also* Microsoft Virtualization; server virtualization  
 Virtualization Management Console, 368, 369  
 Virtualization Service Clients (VSCs), 324, 325  
 Virtualization Service Provider (VSP), 324, 325  
 virtual-to-virtual (V2V) conversion, 367, 374–375  
 VLANs (Virtual Local Area Networks), 255, 304  
 VMBus, 324  
 .vmdk files  
   migration to .vhf file, 361, 374–375  
   P2V conversion on, 367  
 VMS (Virtual Machine Service), 324  
 VMware  
   ESX Server, 356–358  
   management of, 374–375  
   management of virtual assets, 382–383  
   volume recovery, 474  
 Volume Shadow Copy Services (VSS), 367, 506  
 vote system, 483  
 VPN (Virtual Private Network), 28, 30–31  
 VSCs (Virtualization Service Clients), 324, 325  
 VSP (Virtualization Service Provider), 324, 325  
 vulnerability, 321
- ## W
- wastage, 311, 313–314  
 wbadmin.exe, 523  
 WDS. *See* Windows Deployment Services  
 Web application, planning for, 57–59  
 Web farms, 57–58  
 Web Server Role, 477  
 Web site, 174–175  
 weighted path, 468  
 WHQL (Windows Hardware Quality Labs) certification, 210  
 Wide Area Network (WAN), 36  
 WIM (Windows Image Format) file, 446  
 Windows 2003, 303  
 Windows Deployment Services (WDS)  
   automation, scheduling, 54  
   description of, 91–92  
   function of, 43  
   installation, configuration of, 43–53  
   standard server image, 53–54  
   for unattended installs of Windows Server 2008, 76  
 Windows Firewall  
   advanced configuration of, 267–270  
   command line configuration of, 289–290  
   Failover Clustering and, 494  
   management of, 257–266  
   monitoring, 290–291  
 Windows Firewall with Advanced Security  
   description of, 257  
   overview of, 267–270

- Windows Hardware Quality Labs (WHQL)  
certification, 210
- Windows Image Format (WIM) file, 446
- Windows Installer Package, 414–419
- Windows Management Interface (WMI)
- BitLocker Drive Encryption management with, 474
  - code availability, 375
  - server management with, 369
- Windows Process Activation Service (WPAS), 477
- Windows Recovery Environment (WinRE), 521, 522
- Windows Remote Shell, 355
- Windows Search Service, 70
- Windows Security Health Agent (WSHA), 256
- Windows Security Health Validator, 256
- Windows Server 2008
- automated server deployment, 42–57
  - data management tools, 468–471
  - data security features, 471–475
  - edition, selection of, 3–4
  - Eventing, 298–299
  - event/service management
    - improvements, 217
  - Failover Clustering improvements, 481–482
  - Failover Clustering installation on, 484–498
  - full server backup on, 510–519
  - installation of, 5–10
  - installation on parent partition, 323–324
  - roles, adding, 95–98
  - rollback planning, 5
  - virtualization licensing, 4
  - VPN Server, 251
- Windows Server Backup installation on, 506–510
- Windows Server Virtualization Role, installation of, 332–344
- Windows Update, enabling on, 164–166
- WSUS 3.0 SP1 deployment on, 169–171
- See also* server deployment, planning for Windows Server 2008 Datacenter, 4
- Windows Server 2008 Datacenter with Hyper-V, 4
- Windows Server 2008 Enterprise Edition, 4, 390, 456
- Windows Server 2008 Enterprise with Hyper-V, 4
- Windows Server 2008 Itanium, 4
- Windows Server 2008 Standard, 4
- Windows Server 2008 Standard with Hyper-V, 4
- Windows Server 2008 Web, 4
- Windows Server Backup
- data recovery strategies, 520–521
  - design of, 505–506
- Directory Services backup, 523, 542
- Directory Services recovery, 523–527
- full server backup with, 510–519
  - installation of, 506–510
  - object level recovery with, 527–534
  - server recovery, 521–523
- Windows Server Update Services (WSUS)
- 3.0 SP1 Console Only installation, 183–188
  - 3.0 SP1 deployment, 169–171
  - 3.0 SP1 installation, 172–183
  - application patching, 196–199
  - Automatic Updates for clients, 189–196
  - connection to, 188
  - IIS 7.0 components, installation of, 166–169
  - for patch management, 162–163
- Windows Server Virtualization (WSv)
- competition comparison, 356–358
  - installation of, 332–344
  - overview of, 377–379
  - server management, 368–369

- System Center Virtual Machine Manager  
2007, 360–375  
virtual assets management, 381–382  
virtual machine creation methods, 345  
virtual server placement, 358–360  
Windows Share and Storage Management  
Console, 468–469  
Windows Sharepoint Services (WSS)  
3.0 SP1, 476  
for data collaboration, 541  
function of, 476  
IIS 7.0 to host, 59  
installation options, 478–479  
levels of services, 476  
Server Roles/features, prerequisite,  
476–478  
Sharepoint farms, 479–480  
Windows Storage Explorer Console,  
469–470  
Windows Storage Manager for Storage Area  
Networks (SANs) Console, 470–471  
Windows System Resource Manager  
(WSRM)  
enabling, 214–217  
exam preparation for, 227  
functions of, 213  
installing, 421–424  
overview of, 452  
on Server 2008 Enterprise Edition, 456  
Windows Update, 164–166  
Windows Virtualization Manager, 343–344  
Windows Vista
- SCCM 2007 Management Console,  
installing on, 429–434  
SSTP on, 303  
Virtual Server 2005 R2 SP1  
support of, 330  
Windows XP, 250, 303  
Windows XP Professional, 328  
WinRE (Windows Recovery Environment),  
521, 522  
WinRM quickconfig, 355  
Witness Disk, 482–483  
WMI. *See* Windows Management  
Interface  
WMI Provider, 324, 355  
workloads, 313, 314  
workstation, 371–372  
WPAS (Windows Process Activation  
Service), 477  
WSHA (Windows Security Health  
Agent), 256  
WSRM. *See* Windows System Resource  
Manager  
WSS. *See* Windows Sharepoint Services  
WSUS. *See* Windows Server Update  
Services  
WSv. *See* Windows Server Virtualization
- X**  
Xen-enabled Linux Kernels, 326
- Z**  
zones, DNS, 22–24