



BEST DAMN WINDOWS Server 2003 **BOOK** **PERIOD**

**Everything You Need to Know About
Managing a Windows Server 2003 Enterprise**

- Complete Coverage of IP Security: All Models, Protocols, and Components
- Detailed Coverage of Active Directory Infrastructure, Including Administrative Tools, Implementing Active Directory Security, and Access Control
- Step-by-Step Instructions on Planning and Implementing Routing and Remote Access

Susan Snedaker

Register for Free Membership to

s o l u t i o n s @ s y n g r e s s . c o m

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2000*, Brian Caswell and Jay Beale's *Snort 2.0 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy to search web page, providing you with the concise, easy to access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

**BEST
DAMN** **Windows**
Server 2003 **BOOK**
PERIOD

Susan Snedaker

Syngress Publishing, 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®, Syngress®, “Career Advancement Through Skill Enhancement®,” “Ask the Author UPDATE®,” and “Hack Proofing®,” are registered trademarks of Syngress Publishing, Inc. “Syngress: The Definition of a Serious Security Library”™, “Mission Critical™,” and “The Only Way to Stop a Hacker is to Think Like One™” are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY SERIAL NUMBER

001	HJ642HLP MN
002	PO823H7N4C
003	8NJH24589
004	VBP965T5T5
005	CV23GHSES4
006	VB5429IJN6
007	HJJ3EFG6GB
008	29MKFG6932
009	629TGHCXDE
010	IMTGHXWQ39

PUBLISHED BY

Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

The Best Damn Windows Server 2003 Book Period

Copyright © 2004 by Syngress Publishing, 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: 1-931836-12-4

Acquisitions Editor: Jaime Quigley
Page Layout and Art: Patricia Lupien

Cover Designer: Michael Kavish
Indexer: Rich Carlson

Distributed by O'Reilly & Associates in the United States and Canada.



Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly & Associates, Inc. The enthusiasm and work ethic at ORA is incredible and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Lynn Schwartz, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, and Rob Bullington.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack, and Krista Leppiko, for making certain that our vision remains worldwide in scope.

David Buckland, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.



Author

Susan Snedaker (MBA, BA, MCSE, MCT, PM) is Principal Consultant and founder of Virtual Team Consulting, LLC, a consulting firm specializing in start-ups and companies in transition, particularly technology companies. Virtual Team Consulting works with technology start-ups to develop viable business plans in preparation for debt/equity funding or due diligence with venture capital firms. Virtual Team Consulting also provides IT consulting, design and implementation services to businesses of all sizes. The firm assists companies with strategic planning, operations improvement and project management. Through its team of subject matter experts, Virtual Team Consulting also offers financial and change management services to targeted companies.

Prior to founding Virtual Team Consulting in May 2000, Susan held various executive and technical positions with companies including Microsoft, Honeywell, Keane, and Apta Software. As Director of Service Delivery for Keane, she managed 1200+ technical support staff delivering phone and email support for various Microsoft products such as Windows Server operating systems. She has contributed technical chapters to six Syngress Publishing books on Windows and security technologies, and has written and edited technical content for a variety of publications. Susan has also developed and delivered technical content from security to telephony, TCP/IP to wi-fi and just about everything in between (she admits a particular fondness for anything related to TCP/IP).

Susan holds a master's degree in business administration and a bachelor's degree in management from the University of Phoenix; she also holds a certificate in project management from Stanford University. She is a member of the Information Technology Association of Southern Arizona (ITASA).



Special Contributors

Thomas W. Shinder M.D. (MVP, MCSE) is a computing industry veteran who has worked as a trainer, writer, and a consultant for Fortune 500 companies including FINA Oil, Lucent Technologies, and Sealand Container Corporation. Tom was a Series Editor of the Syngress/Osborne Series of Windows 2000 Certification Study Guides and is author of the best selling books *Configuring ISA Server 2000: Building Firewalls with Windows 2000* (Syngress Publishing, ISBN: 1-928994-29-6) and *Dr. Tom Shinder's ISA Server and Beyond* (ISBN: 1-931836-66-3). Tom is the editor of the Brainbuzz.com *Win2k News* newsletter and is a regular contributor to TechProGuild. He is also content editor, contributor and moderator for the World's leading site on ISA Server 2000, www.isaserver.org. Microsoft recognized Tom's leadership in the ISA Server community and awarded him their Most Valued Professional (MVP) award.

Debra Littlejohn Shinder (MCSE) is a technology consultant, trainer, and writer who has authored a number of books on networking, including *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress Publishing (ISBN: 1-931836-65-5), and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP* (ISBN: 1-928994-11-3), the best-selling *Configuring ISA Server 2000* (ISBN: 1-928994-29-6), and *ISA Server and Beyond* (ISBN: 1-931836-66-3). Deb is also a technical editor and contributor to books on subjects such as the Windows 2000 MCSE exams, the CompTIA Security+ exam, and TruSecure's ICSA certification. She edits the Brainbuzz A+ Hardware News and Sunbelt Software's WinXP News and is regularly published in TechRepublic's TechProGuild and Windowsecurity.com. Deb currently specializes in security issues and Microsoft products. She lives and works in the Dallas-Fort Worth area.

Laura E. Hunter (CISSP, MCSE, MCT, MCDBA, MCP, MCP+I, CCNA, A+, Network+, iNet+, CNE-4, CNE-5) is a Senior IT Specialist with the University of Pennsylvania, where she provides network planning, implementation, and troubleshooting services for various business units and schools

within the University. Her specialties include Microsoft Windows NT and 2000 design and implementation, troubleshooting and security topics. As an “MCSE Early Achiever” on Windows 2000, Laura was one of the first in the country to renew her Microsoft credentials under the Windows 2000 certification structure. Laura’s previous experience includes a position as the Director of Computer Services for the Salvation Army and as the LAN administrator for a medical supply firm. She also operates as an independent consultant for small businesses in the Philadelphia metropolitan area and is a regular contributor to the TechTarget family of websites.

Laura has previously contributed to the Syngress Publishing’s *Configuring Symantec Antivirus, Corporate Edition* (ISBN 1-931836-81-7). She has also contributed to several other exam guides in the Syngress Windows Server 2003 MCSE/MCSA DVD Guide and Training System series as a DVD presenter, contributing author, and technical reviewer. Laura holds a bachelor’s degree from the University of Pennsylvania and is a member of the Network of Women in Computer Technology, the Information Systems Security Association, and InfraGard, a cooperative undertaking between the U.S. Government other participants dedicated to increasing the security of United States critical infrastructures.

Chad Todd (MCSE: Security, MCSE, MCSA: Security, MCSA, MCP+I, MCT, CNE, A+, Network+, i-Net+) author of *Hack Proofing Windows 2000 Server* (Syngress, ISBN: 1-931836-49-3) co-owns a training and integration company (Training Concepts, LLC) in Columbia, SC. Chad first certified on Windows NT 4.0 and has been training on Windows operating systems ever since. His specialties include Exchange messaging and Windows security. Chad was awarded MCSE 2000 Charter Member for being one of the first two thousand Windows 2000 MCSEs and MCSA 2002 Charter Member for being one of the first five thousand MCSAs. Chad is a regular contributing author for *Microsoft Certified Professional Magazine*. Chad has worked for companies such as Fleet Mortgage Group, Ikon Office Solutions, and Netbank.

Jeffery A. Martin (MCSE, MCDBA, MCT, MCP+I, MCP, MCNE, CNE, CNA, CNI, CCNA, CCNP, CCI, CCA, CTT, A+, Network+, I-Net+, Project+, Linux+, CIW, ADPM) has been working with computers and computer networks for over 15 years. Jeffery spends most of his time managing

several companies that he owns and consulting for large multinational media companies. He also enjoys working as a technical instructor and training others in the use of technology.

Chris Peiris (MVP, MIT) works as an independent consultant for .NET and EAI implementations. He is currently working with the Commonwealth Bank of Australia. He also lectures on distributed component architectures (.NET, J2EE, and CORBA) at Monash University, Caulfield, Victoria, Australia. Chris was awarded the Microsoft Most Valuable Professional for his contributions to .NET technologies by Microsoft, Redmond. Chris is designing and developing Microsoft solutions since 1995. His expertise lies in developing scalable, high-performance solutions for financial institutions, G2G, B2B, and media groups. Chris has written many articles, reviews, and columns for various online publications including 15Seconds, Developer Exchange (www.devx.com), and Wrox Press. He is co-author of *C# Web Service with .NET Remoting and ASP.NET* and *C# for Java Programmers* (Syngress Publishing, ISBN: 1-931836-54-X), and study guides on MCSA/MCSE Exams 70-290 and Exam 70-298, also from Syngress. Chris frequently presents at professional developer conferences on Microsoft technologies.

His core skills are C++, Java, .NET, C#, VB.NET, Service Oriented Architecture, DNA, MTS, Data Warehousing, WAP, and SQL Server. Chris has a bachelor's in computing, a bachelor of business (accounting), and a masters in information technology. He is currently under taking a PhD on web service management framework. He lives with his family in ACT, Australia.

Martin Grasdal (MCSE+I, MCSE/W2K MCT, CISSP, CTT+, A+) is an independent consultant with over 10 years experience in the computer industry. Martin has a wide range of networking and IT managerial experience. He has been an MCT since 1995 and an MCSE since 1996. His training and networking experience covers a number of products, including NetWare, Lotus Notes, Windows NT, Windows 2000, Windows 2003, Exchange Server, IIS, and ISA Server. As a manager, he served as Director of Web Sites and CTO for BrainBuzz.com, where he was also responsible for all study guide and technical content on the CramSession.com Web sit. Martin currently works actively as a consultant, author, and editor. His recent consulting experience includes contract work for Microsoft as a Technical Contributor to the MCP Program on projects related to server technologies. Martin lives in

Edmonton, Alberta, Canada with his wife Cathy and their two sons. Martin's past authoring and editing work with Syngress has included the following titles: *Configuring and Troubleshooting Windows XP Professional* (ISBN: 1-928994-80-6), *Configuring ISA Server 2000: Building Firewalls for Windows 2000* (ISBN: 1-928994-29-6), and *Dr. Tom Shinder's ISA Server & Beyond: Real World Security Solutions for Microsoft Enterprise Networks* (ISBN: 1-931836-66-3).

Contents

Forewordxxxiii
Chapter 1 Overview of Windows Server 20031
Introduction1
Windows XP/Server 20031
What's New in Windows Server 2003?2
New Features2
New Active Directory Features3
Improved File and Print Services4
Revised IIS Architecture6
Enhanced Clustering Technology6
New Networking and Communications Features7
Improved Security8
Better Storage Management9
Improved Terminal Services9
New Media Services10
XML Web Services11
The Windows Server 2003 Family12
Why Four Different Editions?12
Members of the Family12
Web Edition13
Standard Edition13
Enterprise Edition13
Datacenter Edition14
Licensing Issues14
Product Activation15
Installation and Upgrade Issues16
Common Installation Issues16
Common Upgrade Issues16
Windows Server 2003 Planning Tools and Documentation17
Overview of Network Infrastructure Planning17
Planning Strategies18
Using Planning Tools18
Reviewing Legal and Regulatory Considerations19
Calculating TCO20
Developing a Windows Server 2003 Test Network Environment21
Planning the Test Network22
Exploring the Group Policy Management Console (GMPC)24
Documenting the Planning and Network Design Process25
Creating the Planning and Design Document25
Chapter 2 Using Server Management Tools27
Introduction27
Recognizing Types of Management Tools28
Administrative Tools Menu28
Custom MMC Snap-Ins29
MMC Console Modes29
Command-Line Utilities31
Wizards31
Windows Resource Kit32

The Run As command	.32
Managing Your Server Remotely	.32
Remote Assistance	.32
Using Web Interface for Remote Administration	.33
Remote Desktop for Administration	.34
Administration Tools Pack (adminpak.msi)	.34
Windows Management Instrumentation (WMI)	.35
Using Computer Management to Manage a Remote Computer	.35
Which Tool To Use?	.37
Using Emergency Management Services	.37
Managing Printers and Print Queues	.38
Using the Graphical Interface	.38
Creating a Printer	.39
Sharing a Printer	.39
Adding Printer Drivers for Earlier Operating Systems	.39
Setting Permissions	.40
Managing Print Queues	.41
Managing Printer Pools	.41
Scheduling Printers	.42
Setting Printing Priorities	.42
Using New Command-Line Tools	.43
The Printer Spooler Service	.45
The Internet Printing Protocol	.46
Using the Graphical Interface	.46
Using New Command-Line Utilities	.46
Sc.exe	.47
Schtasks.exe	.47
Setx.exe	.48
Shutdown.exe	.48
Tasklist.exe	.48
Taskkill.exe	.49
Using Wizards to Configure and Manage Your Server	.50
Using the Configure Your Server Wizard and Manage Your Server	.50
Chapter 3 Planning Server Roles and Server Security	.51
Introduction	.51
Understanding Server Roles	.52
Domain Controllers (Authentication Servers)	.54
Active Directory	.54
Operations Master Roles	.55
File and Print Servers	.57
Print Servers	.57
File Servers	.57
DHCP, DNS, and WINS Servers	.57
DHCP Servers	.58
DNS Servers	.58
WINS Servers	.58
Web Servers	.58
Web Server Protocols	.58
Web Server Configuration	.59
Database Servers	.60
Mail Servers	.60
Certificate Authorities	.61
Certificate Services	.61
Application Servers and Terminal Servers	.64
Application Servers	.64

Terminal Servers	.66
Planning a Server Security Strategy	.66
Choosing the Operating System	.66
Security Features	.68
Identifying Minimum Security Requirements for Your Organization	.68
Identifying Configurations to Satisfy Security Requirements	.70
Planning Baseline Security	.70
Customizing Server Security	.70
Securing Servers According to Server Roles	.71
Security Issues Related to All Server Roles	.71
Securing Domain Controllers	.75
Securing File and Print Servers	.76
Securing DHCP, DNS, and WINS Servers	.77
Securing Web Servers	.78
Securing Database Servers	.78
Securing Mail Servers	.79
Securing Certificate Authorities	.79
Securing Application and Terminal Servers	.80
Chapter 4 Security Templates and Software Updates	.81
Introduction	.81
Security Templates	.82
Types of Security Templates	.83
Network Security Settings	.84
Analyzing Baseline Security	.88
Applying Security Templates	.93
Secedit.exe	.93
Group Policy	.94
Security Configuration and Analysis	.95
Software Updates	.95
Install and Configure Software Update Infrastructure	.96
Install and Configure Automatic Client Update Settings	.101
Supporting Legacy Clients	.104
Testing Software Updates	.106
Chapter 5 Managing Physical and Logical Disks	.107
Introduction	.107
Working with Microsoft Disk Technologies	.108
Physical vs Logical Disks	.108
Basic vs Dynamic Disks	.108
Partitions vs Volumes	.110
Partition Types and Logical Drives	.110
Volume Types	.111
Using Disk Management Tools	.115
Using the Disk Management MMC	.115
Using the Command-Line Utilities	.117
Using Diskpart.exe	.117
Using Fsutil.exe	.119
Using Rss.exe	.120
Managing Physical and Logical Disks	.120
Managing Basic Disks	.120
When to Use Basic Disks	.121
Creating Partitions and Logical Drives	.121
Formatting a Basic Volume	.130
Extending a Basic Volume	.132
Managing Dynamic Disks	.133

Converting to Dynamic Disk Status	133
Creating and Using RAID-5 Volumes	146
Optimizing Disk Performance	149
Defragmenting Volumes and Partitions	149
Using the Graphical Defragmenter	150
Using Defrag.exe	154
Defragmentation Best Practices	155
Configuring and Monitoring Disk Quotas	155
Brief Overview of Disk Quotas	155
Enabling and Configuring Disk Quotas	156
Monitoring Disk Quotas	159
Exporting and Importing Quota Settings	160
Disk Quota Best Practices	163
Using Fsutil to Manage Disk Quotas	163
Implementing RAID Solutions	164
Understanding Windows Server 2003 RAID	164
Hardware RAID	165
RAID Best Practices	165
Understanding and Using Remote Storage	166
What is Remote Storage?	166
Storage Levels	167
Relationship of Remote Storage and Removable Storage	167
Setting Up Remote Storage	168
Installing Remote Storage	168
Configuring Remote Storage	171
Using Remote Storage	174
Remote Storage Best Practices	177
Troubleshooting Disks and Volumes	178
Troubleshooting Basic Disks	178
New Disks Are Not Showing Up in the Volume List View	178
Disk Status is Not Initialized or Unknown	179
Disk Status is Failed	180
Troubleshooting Dynamic Volumes	181
Disk Status is Foreign	181
Disk Status is Online (Errors)	182
Disk Status is Offline	182
Disk Status is Data Incomplete	183
Troubleshooting Fragmentation Problems	184
Computer is Operating Slowly	184
The Analysis and Defragmentation Reports Do Not Match the Display	184
My Volumes Contain Unmovable Files	184
Troubleshooting Disk Quotas	184
The Quota Tab is Not There	185
Deleting a Quota Entry Gives you Another Window	185
A User Gets an “Insufficient Disk Space” Message When Adding Files to a Volume	186
Troubleshooting Remote Storage	186
Remote Storage Will Not Install	187
Remote Storage Is Not Finding a Valid Media Type	187
Files Can No Longer Be Recalled from Remote Storage	187
Troubleshooting RAID	187
Mirrored or RAID-5 Volume’s Status is Data Not Redundant	187
Mirrored or RAID-5 Volume’s Status is Failed Redundancy	187
Mirrored or RAID-5 Volume’s Status is Stale Data	188

Chapter 6 Implementing Windows Cluster Services and Network Load	189
Balancing	
Introduction	189
Making Server Clustering Part of Your High-Availability Plan	190
Terminology and Concepts	190
Cluster Nodes	191
Cluster Groups	191
Failover and Failback	192
Cluster Services and Name Resolution	192
How Clustering Works	192
Cluster Models	193
Single Node	193
Single Quorum Device	194
Majority Node Set	194
Server Cluster Deployment Options	196
N-Node Failover Pairs	196
Hot-Standby Server/N+1	197
Failover Ring	199
Random	200
Server Cluster Administration	201
Using the Cluster Administrator Tool	201
Using Command-Line Tools	202
Recovering from Cluster Node Failure	205
Server Clustering Best Practices	206
Hardware Issues	206
Cluster Network Configuration	209
Security	214
Making Network Load Balancing Part of Your High-Availability Plan	224
Terminology and Concepts	225
Hosts/Default Host	225
Load Weight	225
Traffic Distribution	225
Convergence and Heartbeats	226
How NLB Works	227
Relationship of NLB to Clustering	227
Managing NLB Clusters	228
Using the NLB Manager Tool	228
Remote Management	229
Command-Line Tools	229
NLB Error Detection and Handling	232
Monitoring NLB	233
Using the WLBS Cluster Control Utility	234
NLB Best Practices	234
Multiple Network Adapters	234
Protocols and IP Addressing	234
Security	235
Chapter 7 Planning, Implementing, and Maintaining a High-Availability	243
Strategy	
Introduction	243
Understanding Performance Bottlenecks	244
Identifying System Bottlenecks	244
Memory	244
Processor	245
Disk	246

Network Components	246
Using the System Monitor Tool to Monitor Servers	247
Creating a System Monitor Console	257
Using Event Viewer to Monitor Servers	260
Using Service Logs to Monitor Servers	267
Planning a Backup and Recovery Strategy	268
Understanding Windows Backup	268
Types of Backups	269
Determining What to Back Up	272
Using Backup Tools	275
Using the Windows Backup Utility	275
Using the Command-Line Tools	276
Selecting Backup Media	276
Scheduling Backups	277
Restoring from Backup	277
Create a Backup Schedule	279
Planning System Recovery with ASR	283
What Is ASR?	283
How ASR Works	284
Alternatives to ASR	284
Safe Mode Boot	284
Last Known Good Boot Mode	284
ASR As a Last Resort	284
Using the ASR Wizard	285
Performing an ASR Restore	286
Planning for Fault Tolerance	287
Network Fault-Tolerance Solutions	288
Internet Fault-Tolerance Solutions	289
Disk Fault-Tolerance Solutions	289
Server Fault-Tolerance Solutions	289
Chapter 8 Monitoring and Troubleshooting Network Activity	291
Introduction	291
Using Network Monitor	292
Installing Network Monitor	292
Install Network Monitor	292
Basic Configuration	298
Network Monitor Default Settings	299
Configuring Monitoring Filters	299
Configuring Display Filters	300
Interpreting a Trace	301
Perform a Network Trace	301
Monitoring and Troubleshooting Internet Connectivity	304
NAT Logging	304
Name Resolution	310
NetBIOS Name Resolution	311
Using IPConfig to Troubleshoot Name Resolution	312
IP Addressing	314
Client Configuration Issues	315
Network Access Quarantine Control	316
DHCP Issues	317
Monitoring IPSec Connections	318
IPSec Monitor Console	318
Network Monitor	319
Netsh	319

Ipseccmd	320
Netdiag	320
Event Viewer	320
Chapter 9 Active Directory Infrastructure Overview	321
Introduction	321
Introducing Directory Services	322
Terminology and Concepts	323
Directory Data Store	323
Protecting Your Active Directory Data	326
Policy-Based Administration	327
Directory Access Protocol	328
Naming Scheme	328
Installing Active Directory to Create a Domain Controller	331
Install Active Directory	331
Understanding How Active Directory Works	334
Directory Structure Overview	334
Sites	335
Domains	336
Domain Trees	337
Forests	339
Organizational Units	340
Active Directory Components	341
Logical vs. Physical Components	341
Domain Controllers	342
Schema	344
Global Catalog	344
Replication Service	345
Using Active Directory Administrative Tools	347
Graphical Administrative Tools/MMCs	347
Active Directory Users and Computers	349
Active Directory Domains and Trusts	351
Active Directory Sites and Services	354
Command-Line Tools	355
Cacls	355
Cmdkey	356
Csvde	357
Dcgpofix	358
Dsadd	358
Dsget	358
Dsmod	359
Dsmove	359
Ldifde	360
Ntdsutil	362
Whoami	362
Implementing Active Directory Security and Access Control	363
Access Control in Active Directory	364
Set Permissions on AD Objects	366
Role-Based Access Control	367
Authorization Manager	368
Active Directory Authentication	368
Standards and Protocols	368
Kerberos	369
X.509 Certificates	369
LDAP/SSL	369
PKI	369

What's New in Windows Server 2003 Active Directory?	370
New Features Available Only with Windows Server 2003 Domain/Forest Functionality	372
Domain Controller Renaming Tool	372
Domain Rename Utility	372
Forest Trusts	373
Dynamically Links Auxiliary Classes	373
Disabling Classes	373
Replication	373
Raise Domain and Forest Functionality	373
Chapter 10 Working with User, Group, and Computer Accounts	375
Introduction	375
Understanding Active Directory Security Principal Accounts	376
Security Principals and Security Identifiers	376
Tools to View and Manage Security Identifiers	380
Naming Conventions and Limitations	381
Working with Active Directory User Accounts	384
Built-In Domain User Accounts	386
Administrator	387
Guest	387
HelpAssistant	387
SUPPORT_388945a0	387
InetOrgPerson	388
Creating User Accounts	388
Creating Accounts Using Active Directory Users and Computers	388
Create a User Object in Active Directory	389
Creating Accounts Using the DSADD Command	390
Managing User Accounts	393
Personal Information Tabs	393
Account Settings	395
Terminal Services Tabs	398
Security-Related Tabs	400
Working with Active Directory Group Accounts	403
Group Types	404
Security Groups	404
Distribution Groups	404
Group Scopes in Active Directory	405
Universal	405
Global	405
Domain Local	406
Built-In Group Accounts	406
Default Groups in Builtin Container	407
Default Groups in Users Container	407
Creating Group Accounts	408
Creating Groups Using Active Directory Users and Computers	408
Creating Groups Using the DSADD Command	409
Managing Group Accounts	410
Working with Active Directory Computer Accounts	415
Creating Computer Accounts	415
Creating Computer Accounts by Adding a Computer to a Domain	416
Creating Computer Accounts Using Active Directory Users and Computers	417
Creating Computer Accounts Using the DSADD Command	419

Managing Computer Accounts	420
Managing Multiple Accounts	423
Implementing User Principal Name Suffixes	424
Add and Use Alternative UPN Suffixes	424
Moving Account Objects in Active Directory	425
Moving Objects with Active Directory Users and Computers	425
Moving Objects with the DSMOVE Command	426
Moving Objects with the MOVETREE Command	427
Install MOVETREE with AD Support Tools	428
Troubleshooting Problems with Accounts	429
Chapter 11 Creating User and Group Strategies	431
Introduction	431
Creating a Password Policy for Domain Users	432
Creating an Extensive Defense Model	432
Strong Passwords	433
System Key Utility	433
Defining a Password Policy	433
Create a domain password policy	434
Modifying a Password Policy	435
Applying an Account Lockout Policy	436
Create an account lockout policy	436
Creating User Authentication Strategies	437
Need for Authentication	438
Single Sign-On	438
Interactive Logon	438
Network Authentication	438
Authentication Types	439
Kerberos	439
Understanding the Kerberos Authentication Process	440
Secure Sockets Layer/Transport Layer Security	440
NT LAN Manager	441
Digest Authentication	442
Passport Authentication	442
Educating Users	442
Smart Card Authentication	443
Planning a Security Group Strategy	443
Security Group Best Practices	443
Designing a Group Strategy for a Single Domain Forest	443
Designing a Group Strategy for a Multiple Domain Forest	445
Chapter 12 Working with Forests and Domains	449
Introduction	449
Understanding Forest and Domain Functionality	450
The Role of the Forest	450
New Forestwide Features	450
New Domainwide Features	454
Domain Trees	456
Forest and Domain Functional Levels	456
Domain Functionality	457
Forest Functionality	460
Raising the Functional Level of a Domain and Forest	462
Domain Functional Level	463
Verify the domain functional level	463

Raise the domain functional level	463
Forest Functional Level	464
Verify the forest functional level	464
Raise the forest functional level	464
Optimizing Your Strategy for Raising Functional Levels	465
Creating the Forest and Domain Structure	466
Deciding When to Create a New DC	466
Installing Domain Controllers	467
Creating a Forest Root Domain	467
Creating a New Domain Tree in an Existing Forest	469
Create a new domain tree in an existing forest	469
Creating a New Child Domain in an Existing Domain	470
Creating a New DC in an Existing Domain	471
Create a new domain controller in an existing domain using the conventional across-the-network method	471
Create a new domain controller in an existing domain using the new system state backup method	472
Assigning and Transferring Master Roles	475
Locate the Schema Operations Master	476
Transfer the Schema Operations Master Role	477
Locate the Domain Naming Operations Master	478
Transfer the Domain Naming Master Role	479
Locate the Infrastructure, RID and PDC Operations Masters	479
Transfer the Infrastructure, RID and PDC Master Roles	480
Seize the FSMO Master Roles	480
Using Application Directory Partitions	483
Administer Application Directory Partitions	483
Establishing Trust Relationships	484
Direction and Transitivity	484
Types of Trusts	486
Restructuring the Forest and Renaming Domains	486
Domain Rename Limitations	486
Domain Rename Limitations in a Windows 2000 Forest	486
Domain Rename Limitations in a Windows Server 2003 Forest	487
Domain Rename Dependencies	487
Domain Rename Conditions and Effects	488
Rename a Windows Server 2003 Domain Controller	489
Implementing DNS in the Active Directory Network Environment	490
DNS and Active Directory Namespaces	490
DNS Zones and Active Directory Integration	491
Configuring DNS Servers for Use with Active Directory	491
Integrating an Existing Primary DNS Server with Active Directory	492
Creating the Default DNS Application Directory Partitions	493
Using dnscmd to Administer Application Directory Partitions	493
Securing Your DNS Deployment	495
Chapter 13 Working with Trusts and Organizational Units	495
Introduction	495
Working with Active Directory Trusts	496
Types of Trust Relationships	496
Default Trusts	496
Shortcut Trust	497
Realm Trust	497
External Trust	497
Forest Trust	498

Creating, Verifying, and Removing Trusts	499
Create a transitive, one-way incoming realm trust	499
Securing Trusts Using SID Filtering	499
Understanding the Role of Container Objects	500
Creating and Managing Organizational Units	500
Create an Organizational Unit	501
Applying Group Policy to OUs	502
Delegating Control of OUs	503
Planning an OU Structure and Strategy for Your Organization	503
Delegation Requirements	504
Delegate authority for an OU	504
Security Group Hierarchy	504
Chapter 14 Working with Active Directory Sites	507
Introduction	507
Understanding the Role of Sites	508
Replication	508
Authentication	508
Distribution of Services Information	508
Relationship of Sites to Other Active Directory Components	510
Relationship of Sites and Domains	510
Physical vs. Logical Structure of the Network	510
The Relationship of Sites and Subnets	511
Creating Sites and Site Links	511
Site Planning	511
Criteria for Establishing Separate Sites	511
Creating a Site	512
Create a new site	512
Renaming a Site	513
Rename a new site	513
Creating Subnets	513
Create subnets	514
Associating Subnets with Sites	514
Associate subnets with sites	514
Creating Site Links	514
Create site links	515
Configuring Site Link Cost	517
Configure site link costs	517
Site Replication	518
Types of Replication	518
Intra-site Replication	518
Inter-site Replication	520
Planning, Creating, and Managing the Replication Topology	520
Planning Replication Topology	520
Creating Replication Topology	521
Managing Replication Topology	521
Configuring Replication between Sites	522
Configuring Replication Frequency	522
Configuring Site Link Availability	522
Configuring Site Link Bridges	523
Configuring Bridgehead Servers	524
Troubleshooting Replication Failure	524
Troubleshooting Replication	524
Using Replication Monitor	525

Using Event Viewer	526
Using Support Tools	527
Chapter 15 Working with Domain Controllers	529
Introduction	529
Planning and Deploying Domain Controllers	529
Understanding Server Roles	530
Function of Domain Controllers	530
Determining the Number of Domain Controllers	531
Using the Active Directory Installation Wizard	532
Creating Additional Domain Controllers	533
Upgrading Domain Controllers to Windows Server 2003	536
Placing Domain Controllers within Sites	537
Backing Up Domain Controllers	538
Restoring Domain Controllers	538
Managing Operations Masters	539
Chapter 16 Working with Global Catalog Servers and Schema	541
Introduction	541
Working with the Global Catalog and GC Servers	542
Functions of the GC	542
UPN Authentication	542
Directory Information Search	543
Universal Group Membership Information	544
Customizing the GC Using the Schema MMC Snap-In	544
Setup Active Directory Schema MMC Snap-in	545
Creating and Managing GC Servers	545
Understanding GC Replication	546
Universal Group Membership	546
Attributes in GC	547
Placing GC Servers within Sites	547
Bandwidth and Network Traffic Considerations	548
Universal Group Caching	548
Troubleshooting GC Issues	549
Working with the Active Directory Schema	550
Understanding Schema Components	550
Classes	551
Attributes	552
Naming of Schema Objects	555
Working with the Schema MMC Snap-In	556
Modifying and Extending the Schema	557
Deactivating Schema Classes and Attributes	558
Create and deactivate classes or attributes	558
Troubleshooting Schema Issues	559
Chapter 17 Working with Group Policy in an Active Directory Environment	561
Introduction	561
Understanding Group Policy	562
Terminology and Concepts	562
Local and Non-Local Policies	562
User and Computer Policies	563
Group Policy Objects	565
Scope and Application Order of Policies	565
Group Policy Integration in Active Directory	567
Group Policy Propagation and Replication	567
Planning a Group Policy Strategy	568
Using RSoP Planning Mode	568

Opening RSoP in Planning Mode	568
Reviewing RSoP Results	570
Strategy for Configuring the User Environment	571
Strategy for Configuring the Computer Environment	572
Run an RSoP Planning Query	573
Implementing Group Policy	576
The Group Policy Object Editor MMC	576
Creating, Configuring, and Managing GPOs	577
Creating and Configuring GPOs	577
Naming GPOs	578
Managing GPOs	578
Configuring Application of Group Policy	579
General	579
Links	580
Security	580
WMI Filter	581
Delegating Administrative Control	581
Verifying Group Policy	582
Delegate Control for Group Policy to a Non-Administrator	582
Performing Group Policy Administrative Tasks	584
Automatically Enrolling User and Computer Certificates	584
Redirecting Folders	586
Configuring User and Computer Security Settings	588
Computer Configuration	588
User Configuration	589
Redirect the My Documents Folder	589
Using Software Restriction Policies	591
Setting Up Software Restriction Policies	591
Software Policy Rules	592
Precedence of Policies	593
Best Practices	593
Applying Group Policy Best Practices	594
Troubleshooting Group Policy	595
Using RSoP	596
Using gpresult.exe	597
Run an RSoP Query in Logging Mode	599
Chapter 18 Deploying Software via Group Policy	601
Introduction	601
Understanding Group Policy Software Installation Terminology and Concepts	602
Group Policy Software Installation Concepts	602
Assigning Applications	603
Publishing Applications	603
Document Invocation	604
Application Categories	605
Group Policy Software Deployment vs. SMS Software Deployment	605
Group Policy Software Installation Components	605
Windows Installer Packages (.msi)	606
Transforms (.mst)	606
Patches and Updates (.msp)	607
Application Assignment Scripts (.aas)	607
Deploying Software to Users	607
Deploying Software to Computers	608

Using Group Policy Software Installation to Deploy Applications	.608
Preparing for Group Policy Software Installation	.609
Creating Windows Installer Packages	.609
Using .zap Setup Files	.610
Publish Software Using a .ZAP File	.611
Creating Distribution Points	.611
Working with the GPO Editor	.611
Opening or Creating a GPO for Software Deployment	.612
Assigning and Publishing Applications	.612
Assign Software to a Group	.613
Configuring Software Installation Properties	.614
The General Tab	.614
The Advanced Tab	.615
The File Extensions Tab	.615
The Categories Tab	.616
Upgrading Applications	.616
Configuring Required Updates	.617
Removing Managed Applications	.618
Managing Application Properties	.619
Categorizing Applications	.621
Adding and Removing Modifications for Application Packages	.622
Apply a Transform to a Software Package	.622
Troubleshooting Software Deployment	.623
Verbose Logging	.624
Software Installation Diagnostics Tool	.625
Chapter 19 Ensuring Active Directory Availability	.627
Introduction	.627
Understanding Active Directory Availability Issues	.628
The Active Directory Database	.628
Data Modification to the Active Directory Database	.629
The Tombstone and Garbage Collection Processes	.630
System State Data	.631
Fault Tolerance and Performance	.631
Performing Active Directory Maintenance Tasks	.631
Defragmenting the Database	.631
The Offline Defragmentation Process	.631
Perform an Offline Defragmentation of the Active Directory Database	.632
Moving the Database or Log Files	.633
Monitoring the Database	.636
Using Event Viewer to Monitor Active Directory	.636
Using the Performance Console to Monitor Active Directory	.637
Use System Monitor to Monitor Active Directory	.639
Backing Up and Restoring Active Directory	.640
Backing Up Active Directory	.641
Backing Up at the Command Line	.641
Restoring Active Directory	.642
Directory Services Restore Mode	.642
Normal Restore	.642
Authoritative Restore	.647
Primary Restore	.648
Troubleshooting Active Directory Availability	.649
Setting Logging Levels for Additional Detail	.649
Using Ntdsutil Command Options	.649

Using the Integrity Command	.649
Using the recover Command	.651
Using the Semantic Database Analysis Command	.653
Using the esentutl Command	.656
Changing the Directory Services Restore Mode Password	.658
Chapter 20 Planning, Implementing, and Maintaining a Name Resolution Strategy	.659
Introduction	.659
Planning for Host Name Resolution	.660
Install Windows Server 2003 DNS Service and Configure Forward and Reverse Lookup Zones	.663
Designing a DNS Namespace	.666
Host Naming Conventions and Limitations	.666
Supporting Multiple Namespaces	.668
Planning DNS Server Deployment	.672
Planning the Number of DNS Servers	.673
Planning for DNS Server Capacity	.673
Planning DNS Server Placement	.674
Planning DNS Server Roles	.675
Planning for Zone Replication	.678
Active Directory-integrated Zone Replication Scope	.679
Security for Zone Replication	.682
General Guidelines for Planning for Zone Replication	.682
Planning for Forwarding	.683
Conditional Forwarding	.684
General Guidelines for Using Forwarders	.685
DNS/DHCP Interaction	.686
Security Considerations for DDNS and DHCP	.687
Aging and Scavenging of DNS Records	.689
Windows Server 2003 DNS Interoperability	.690
BIND and Other DNS Server Implementations	.690
Zone Transfers with BIND	.693
Supporting AD with BIND	.694
Split DNS Configuration	.694
Interoperability with WINS	.696
DNS Security Issues	.699
Common DNS Threats	.700
Securing DNS Deployment	.702
DNS Security Levels	.702
General DNS Security Guidelines	.704
Monitoring DNS Servers	.706
Testing DNS Server Configuration with the DNS Console Monitoring Tab	.706
Debug Logging	.707
Event Logging	.708
Monitoring DNS Server Using the Performance Console	.708
Command-line Tools for Maintaining and Monitoring DNS Servers	.709
Planning for NetBIOS Name Resolution	.710
Understanding NETBIOS Naming	.710
NetBIOS Name Resolution Process	.711
Understanding the LMHOSTS File	.711
Understanding WINS	.711
What's New for WINS in Windows Server 2003	.712
Planning WINS Server Deployment	.713
Server Number and Placement	.713
Planning for WINS Replication	.714

Replication Partnership Configuration	716
Replication Models	719
WINS Issues	722
Static WINS Entries	722
Multihomed WINS Servers	723
Client Configuration	724
Preventing Split WINS Registrations	726
Performance Issues	726
Security Issues	730
Planning for WINS Database Backup and Restoration	731
Troubleshooting Name Resolution Issues	732
Troubleshooting Host Name Resolution	733
Issues Related to Client Computer Configuration	734
Issues Related to DNS Services	735
Troubleshooting NetBIOS Name Resolution	736
Issues Related to Client Computer Configuration	737
Issues Related to WINS Servers	737
Chapter 21 Planning, Implementing, and Maintaining the TCP/IP Infrastructure	741
Introduction	741
Understanding Windows 2003 Server Network Protocols	742
The Multiprotocol Network Environment	742
What's New in TCP/IP for Windows Server 2003	742
IGMPv3	743
IPv6	743
Alternate Configuration	744
Automatic Determination of Interface Metric	744
Planning an IP Addressing Strategy	746
Analyzing Addressing Requirements	746
Creating a Subnetting Scheme	746
Troubleshooting IP Addressing	747
Client Configuration Issues	747
DHCP Issues	748
Transitioning to IPv6	749
IPv6 Utilities	750
Install TCP/IP Version 6	750
6to4 Tunneling	754
IPv6 Helper Service	754
The 6bone	754
Teredo (IPv6 with NAT)	754
Planning the Network Topology	755
Analyzing Hardware Requirements	755
Planning the Placement of Physical Resources	755
Planning Network Traffic Management	756
Monitoring Network Traffic and Network Devices	756
Using System Monitor	756
Determining Bandwidth Requirements	757
Optimizing Network Performance	757
Chapter 22 Planning, Implementing, and Maintaining a Routing Strategy	759
Introduction	759
Understanding IP Routing Basics	760
Routing Tables	762
Static versus Dynamic Routing	763
Gateways	764
Routing Protocols	764
Using Netsh Commands	770

Evaluating Routing Options	772
Selecting Connectivity Devices	772
Switches	775
Routers	777
Windows Server 2003 As a Router	778
Configure a Windows Server 2003 Computer As a Static Router	779
Configure RIP Version 2	780
Security Considerations for Routing	782
Analyzing Requirements for Routing Components	783
Simplifying Network Topology to Provide Fewer Attack Points	784
Minimizing the Number of Network Interfaces and Routes	785
Minimizing the Number of Routing Protocols	785
Router-to-Router VPNs	786
Install and Enable Windows Server 2003 VPN Server	786
Set Up Windows Server 2003 As Router-to-Router VPN Server	787
Packet Filtering and Firewalls	788
Logging Level	789
Troubleshooting IP Routing	790
Identifying Troubleshooting Tools	790
Common Routing Problems	792
Interface Configuration Problems	792
RRAS Configuration Problems	792
Routing Protocol Problems	793
TCP/IP Configuration Problems	794
Routing Table Configuration Problems	794
Chapter 23 Planning, Implementing, and Maintaining Internet Protocol	
Security	795
Introduction	795
Understanding IP Security (IPSec)	796
How IPSec Works	797
Securing Data in Transit	797
IPSec Cryptography	797
IPSec Modes	798
Tunnel Mode	798
Transport Mode	798
IPSec Protocols	798
Determine IPSec Protocol	798
Additional Protocols	800
IPSec Components	801
IPSec Policy Agent	801
IPSec Driver	802
IPSec and IPv6	802
Deploying IPSec	802
Determining Organizational Needs	802
Security Levels	803
Managing IPSec	804
Using the IP Security Policy Management MMC Snap-in	804
Install the IP Security Policy Management Console	804
Using the netsh Command-line Utility	805
Default IPSec Policies	805
Client (Respond Only)	806
Server (Request Security)	806
Secure Server (Require Security)	806
Custom Policies	807
Customize IP Security Policy	807

Using the IP Security Policy Wizard	808
Create an IPSec Policy with the IP Security Policy Wizard	808
Defining Key Exchange Settings	811
Managing Filter Lists and Filter Actions	812
Assigning and Applying Policies in Group Policy	812
Active Directory Based IPSec Policies	812
IPSec Monitoring	813
Using the netsh Utility for Monitoring	813
Using the IP Security Monitor MMC Snap-in	814
Troubleshooting IPSec	814
Using netdiag for Troubleshooting Windows Server 2003 IPSec	814
Viewing Policy Assignment Information	815
Viewing IPSec Statistics	815
Using Packet Event Logging to Troubleshoot IPSec	817
Using IKE Detailed Tracing to Troubleshoot IPSec	818
Using the Network Monitor to Troubleshoot IPSec	819
Disabling TCP/IP and IPSec Hardware Acceleration to Solve IPSec Problems	820
Addressing IPSec Security Considerations	820
Strong Encryption Algorithm (3DES)	820
Firewall Packet Filtering	821
Diffie-Hellman Groups	821
Pre-shared Keys	821
Advantages and Disadvantages of Pre-shared Keys	822
Considerations when Choosing a Pre-shared Key	822
Soft Associations	822
Security and RSoP	822
Chapter 24 Planning, Implementing, and Maintaining a Public Key Infrastructure	825
Introduction	825
Planning a Windows Server 2003 Certificate-Based PKI	826
Understanding Public Key Infrastructure	826
The Function of the PKI	827
Components of the PKI	827
Understanding Digital Certificates	827
User Certificates	828
Machine Certificates	828
Application Certificates	828
Understanding Certification Authorities	828
CA Hierarchy	829
How Microsoft Certificate Services Works	829
Install Certificate Services	830
Implementing Certification Authorities	830
Configure a Certification Authority	831
Analyzing Certificate Needs within the Organization	833
Determining Appropriate CA Type(s)	833
Enterprise CAs	834
Stand-Alone CAs	834
Planning the CA Hierarchy	835
Planning CA Security	836
Certificate Revocation	837
Planning Enrollment and Distribution of Certificates	838
Certificate Templates	838
Certificate Requests	841
Auto-Enrollment Deployment	842
Role-Based Administration	843

Implementing Smart Card Authentication in the PKI	843
How Smart Card Authentication Works	843
Deploying Smart Card Logon	844
Smart Card Readers	844
Smart Card Enrollment Station	845
Using Smart Cards To Log On to Windows	845
Implement and Use Smart Cards	845
Using Smart Cards for Remote Access VPNs	847
Using Smart Cards To Log On to a Terminal Server	848
Chapter 25 Planning, Implementing, Maintaining Routing and Remote Access	849
Introduction	850
Planning the Remote Access Strategy	850
Analyzing Organizational Needs	850
Analyzing User Needs	850
Selecting Remote Access Types To Allow	851
Dial-In	851
VPN	851
Wireless Remote Access	851
Addressing Dial-In Access Design Considerations	852
Allocating IP Addresses	852
Static Address Pools	852
Using DHCP for Addressing	852
Using APIPA	852
Determining Incoming Port Needs	853
Multilink and BAP	853
Selecting an Administrative Model	854
Access by User	854
Access by Policy	854
Configuring the Windows 2003 Dial-up RRAS Server	855
Configuring RRAS Packet Filters	855
RRAS Packet Filter Configuration	855
Addressing VPN Design Considerations	858
Selecting VPN Protocols	858
Client Support	858
Data Integrity and Sender Authentication	859
PKI Requirements	859
Installing Machine Certificates	859
Configuring Firewall Filters	859
PPP Multilink and Bandwidth Allocation Protocol (BAP)	860
PPP Multilink Protocol	861
BAP Protocols	861
Addressing Wireless Remote Access Design Considerations	862
The 802.11 Wireless Standards	862
Using IAS for Wireless Connections	862
Configuring Remote Access Policies for Wireless Connections	863
Create a Policy for Wireless Access	863
Multiple Wireless Access Points	863
Placing CA on VLAN for New Wireless Clients	863
Configuring WAPs as RADIUS Clients	864
Planning Remote Access Security	864
Domain Functional Level	864
Selecting Authentication Methods	864
Disallowing Password-Based Connections (PAP, SPAP, CHAP, MS-CHAP v1)	865
Disable Password-Based Authentication Methods	865
Using RADIUS/IAS vs. Windows Authentication	865

Selecting the Data Encryption Level	866
Using Callback Security	866
Managed Connections	867
Mandating Operating System/File System	867
Using Smart Cards for Remote Access	867
Configuring Wireless Security Protocols	867
Configure Wireless Networking	870
RRAS NAT Services	873
Configure NAT and Static NAT Mapping	875
ICMP Router Discovery	877
Configure ICMP Router Discovery	877
Creating Remote Access Policies	878
Policies and Profiles	878
Authorizing Remote Access	879
Authorizing Access By Group	879
Restricting Remote Access	880
Restricting by User/Group Membership	880
Restricting by Type of Connection	880
Restricting by Time	881
Restricting by Client Configuration	881
Restricting Authentication Methods	881
Restricting by Phone Number or MAC Address	882
Controlling Remote Connections	882
Controlling Idle Timeout	882
Controlling Maximum Session Time	883
Controlling Encryption Strength	883
Controlling IP Packet Filters	883
Controlling IP Address for PPP Connections	884
Troubleshooting Remote Access Client Connections	884
Troubleshooting Remote Access Server Connections	888
Configuring Internet Authentication Services	891
Configure IAS	892
Chapter 26 Managing Web Servers with IIS 6.0	895
Introduction	895
Installing and Configuring IIS 6.0	896
Pre-Installation Checklist	896
Internet Connection Firewall	896
Installation Methods	897
Using the Configure Your Server Wizard	897
Using the Add or Remove Programs Applet	899
Using Unattended Setup	899
Installation Best Practices	900
What's New in IIS 6.0?	900
New Security Features	900
Advanced Digest Authentication	900
Server-Gated Cryptography (SGC)	901
Selectable Cryptographic Service Provider (CSP)	901
Configurable Worker Process Identity	901
Default Lockdown Status	902
New Authorization Framework	902
New Reliability Features	902
Health Detection	903
New Request Processing Architecture: HTTP.SYS Kernel Mode Driver	903

Other New Features	904
ASP.NET and IIS Integration	904
Unicode Transformation Format-8 (UTF-8)	904
XML Metabase	905
Managing IIS 6.0	905
Performing Common Management Tasks	906
Site Setup	906
Common Administrative Tasks	914
Enable Health Detection	920
Managing IIS Security	920
Configuring Authentication Settings	921
Troubleshooting IIS 6.0	923
Troubleshooting Content Errors	923
Static Files Return 404 Errors	923
Dynamic Content Returns a 404 Error	924
Sessions Lost Due to Worker Process Recycling	924
Configure Worker Process Recycling	924
ASP.NET Pages are Returned as Static Files	924
Troubleshooting Connection Errors	924
503 Errors	925
Extend The Queue Length of An Application Pool	925
Extend The Error Count and Timeframe	925
Clients Cannot Connect to Server	925
401 Error—Sub Authentication Error	926
Client Requests Timing Out	926
Troubleshooting Other Errors	926
File Not Found Errors for UNIX and Linux Files	926
ISAPI Filters Are Not Automatically Visible as Properties of the Web Site	927
The Scripts and Msadc Virtual Directories Are Not Found in IIS 6.0	927
Using New IIS Command-Line Utilities	927
iisweb.vbs	927
iisvdir.vbs	927
iisftp.vbs	928
iisftpr.vbs	928
iisback.vbs	928
iiscnfg.vbs	928
Chapter 27 Managing and Troubleshooting Terminal Services	929
Introduction	929
Understanding Windows Terminal Services	930
Terminal Services Components	930
Remote Desktop for Administration	930
Remote Assistance	931
The Terminal Server Role	932
Using Terminal Services Components for Remote Administration	933
Configuring RDA	933
Enabling RDA Access	933
Remote Desktop Security Issues	934
Using Remote Assistance	935
Configuring Remote Assistance for Use	935
Asking for Assistance	935
Managing Open Invitations	936
Remote Assistance Security Issues	937
Installing and Configuring the Terminal Server Role	938
Install the Terminal Server Role	938
Install Terminal Server Licensing	939

Using Terminal Services Client Tools	940
Installing and Using the Remote Desktop Connection (RDC) Utility	940
Installing the Remote Desktop Connection Utility	941
Launching and Using the Remote Desktop Connection Utility	941
Configuring the Remote Desktop Connection Utility	942
Installing and Using the Remote Desktops MMC Snap-In	946
Install the Remote Desktops MMC Snap-In	947
Configure a New Connection in the RD MMC	947
Configure a Connection's Properties	948
Connecting and Disconnecting	949
Installing and Using the Remote Desktop Web Connection Utility	949
Install the Remote Desktop Web Connection Utility	949
Using the Remote Desktop Web Connection Utility from a Client	951
Using Terminal Services Administrative Tools	953
Use Terminal Services Manager to Connect to Servers	953
Manage Users with the Terminal Services Manager Tool	954
Manage Sessions with the Terminal Services Manager Tool	954
Manage Processes with the Terminal Services Manager Tool	955
Using the Terminal Services Configuration Tool	956
Understanding Listener Connections	956
Modifying the Properties of an Existing Connection	957
Terminal Services Configuration Server Settings	965
User Account Extensions	966
The Terminal Services Profile Tab	966
The Sessions Tab	967
The Environment Tab	968
The Remote Control Tab	969
Using Group Policies to Control Terminal Services Users	970
Using the Terminal Services Command-Line Tools	971
Use Terminal Services Manager to Reset a Session	972
Troubleshooting Terminal Services	972
Not Automatically Logged On	973
"This Initial Program Cannot Be Started"	973
Clipboard Problems	973
License Problems	974
Index	975

Foreword

Any IT professional who's been in the business more than 15 minutes knows that the only constant is change. Staying up-to-date on computing technologies is an unrelenting process. Those that thrive in this industry are those that enjoy continuous learning and new challenges. That said, it's still a daunting task to keep on top of fast-changing technology. From worms and viruses to storage area networks to Wi-Fi, today's IT professional has to constantly take in vast amounts of data, sort through it for relevant pieces, and figure out how to apply it to his or her own network.

Windows Server 2003 is based on the technologies introduced or enhanced in Windows 2000. This updated operating system contains all the technological updates you'd expect, as well as a determined effort by Microsoft to improve security. Out of the box, Windows Server 2003 is more secure than any previous Microsoft operating system. It's locked down, it doesn't install unnecessary components, and it requires activation or enabling of some key features that are installed by default. Overall, this operating system is the most stable, secure operating system Microsoft has built. The focus on security is evident and anyone running a Windows-based network should take a serious look at upgrading to this new version – not only to take advantage of the new features such as support for the latest protocols, but to improve overall security.

This book is designed to give you the best of the best. Each chapter was specifically selected to provide both the depth and breadth needed to work effectively with Windows Server 2003 without extraneous or irrelevant information. Of course, it would be easy to fill volumes on Windows Server 2003 and the technologies that go into this operating system. What we've done instead is focus on what you really

need to know to plan, install, manage and secure a Windows Server 2003 network. You won't find arcane references to the technical specifications of RFC 2460 (IPv6 for those of you who were about to jump to the IETF website or geekier still, those who have the RFC index file on their desktop). What you will find is accurate, focused technical information you can use today to manage your Windows Server 2003 systems and networks. You'll find a practical blend of technical information and step-by-step instructions on common Windows Server 2003 tasks. You can read this book from cover to cover and become highly knowledgeable about Windows Server 2003, or you can flip to specific chapters as references for particular tasks. Either way, you'll find this is the best damn Windows Server 2003 book . . . period.

— Susan Snedaker

Many thanks for the good-natured guidance from my editor, Jaime Quigley, at Syngress. Thanks also to my fine friend and mentor, Nick Mammana, who long ago taught me it's both what you say and how you say it that matter. And last, but certainly not least, thanks to Lisa Mainz for being such a techno-geek. I've learned a lot watching you break the rules.

Overview of Windows Server 2003

In this chapter:

- **What's New in Windows Server 2003?**
- **The Windows Server 2003 Family**
- **Licensing Issues**
- **Installation and Upgrade Issues**
- **Planning Tools and Documentation**

Introduction

The latest incarnation of Microsoft's server product, Windows Server 2003, brings many new features and improvements that make the network administrator's job easier. This chapter will briefly summarize what's new in 2003 and introduce you to the four members of the Windows Server 2003 family: the Web Edition, the Standard Edition, the Enterprise Edition, and the Datacenter Edition. We'll also discuss how licensing works with Windows Server 2003, and provide a heads up on some of the issues you might encounter when installing the new OS or upgrading from Windows 2000. We'll look at the tools and documentation that come with Windows Server 2003 to familiarize you with new features in this version of the Microsoft operation system.

Windows XP/Server 2003

Windows XP and Windows Server 2003 are based on the same code and are the client and server editions of the same OS, with the same relationship to one another as Windows 2000 Professional and Windows 2000 Server.

Windows XP is available in four 32-bit editions:

- Windows XP Home Edition
- Windows XP Professional
- Windows XP Media Center Edition
- Windows XP Tablet PC Edition

There is also a 64-bit version of XP, designed to run on the Itanium processor. Windows Server 2003 comes in four editions (discussed later in this chapter):

- Windows Server 2003 Web Edition
- Standard Edition
- Enterprise Edition
- Datacenter Server

Server 2003 comes in both 32-bit and 64-bit versions.

Windows XP introduced a new variation to the 9x style GUI. The new interface is called LUNA and is also used by Windows Server 2003. The idea behind LUNA is to clean up the desktop and access everything needed from the Start menu. If you don't care for LUNA, both XP and Server 2003 also support the classic Windows 9x/NT 4.0 style GUI.

What's New in Windows Server 2003?

Windows Server 2003 improves upon previous versions of Windows in the areas of availability, reliability, security, and scalability. Windows 2003 is designed to allow customers to do more with less. According to Microsoft, companies that have deployed Windows 2003 have been able to operate with up to 30 percent greater efficiency in the areas of application development and administrative overhead.

New Features

Microsoft has enhanced most of the features carried over from Windows 2000 Server and has added some new features for Windows Server 2003. For example:

- Active Directory has been updated to improve replication, management, and migrations.
- File and Print services have been updated to make them more dependable and quicker.
- The number of nodes supported in clustering has been increased and new tools have been added to aid in cluster management.
- Terminal Server better supports using local resources when using the Remote Desktop Protocol.
- IIS 6.0, Media Services 9.0, and XML services have been added to Windows Server 2003.

- New networking technologies and protocols are supported, including Simple Object Access Protocol (SOAP), Web Distributed Authoring and Versioning (WebDAV), IPv6, wireless networking, fiber channel, and automatic configuration for multiple networks.
- New command-line tools have been added for easier administration.
- Software Restriction Policies allow administrators to control which applications can be run.
- All features of Windows have been updated to reflect Microsoft's security initiative.

New Active Directory Features

Active Directory was first introduced in Windows 2000 and Microsoft has made improvements to AD in Windows Server 2003. Windows 2003 enhances the management of Active Directory. There are more AD management tools now and the tools are easier than ever to use. Microsoft has made it painless to deploy Active Directory in Windows 2003. The migration tools have been greatly improved to make way for seamless migrations.

In the corporate world where mergers and acquisitions are common, things change all the time. With Windows Server 2003, you can rename your domains, a feature missing from Windows 2000. You can also change the NetBIOS name, the DNS name, or both.

Another problem with changes in the business environment is the need to configure trust relationships. With Windows 2000, if two companies merge and each has a separate Active Directory, they have to either set up manual nontransitive trusts between all of their domains or collapse one forest into the other. Neither of these is an ideal choice and is prone to error. The trusts are easy enough to set up, but then you lose the benefits of being in a single forest. Collapsing forests can require a lot of work, depending on the environment.

Windows Server 2003 Active Directory now supports forest-level trusts. By setting the trusts at the forest roots, you enable cross-forest authentication and cross-forest authorization. Cross-forest authentication provides a single sign-on experience by allowing users in one forest to access machines in another forest via NTLM or Kerberos (Kerberos is the preferred method, if all systems support it). Cross-forest authorization allows assigning permissions for users in one forest to resources in another forest. Permissions can be assigned to the user ID or through groups.

Not all improvements have to do with mergers and multiple forests. In the past, it was common practice for companies with many offices spread out geographically to build their domain controllers locally and ship them to the remote offices. This was because of replication issues. When a new domain controller is created, it must pull a full copy of the Active Directory database from another domain controller. This full replication can easily oversaturate a slow network link. However, with Server 2003, you can create a new domain controller and pull the Active Directory information from your backup media. The newly created domain controller now only has to replicate the changes that have occurred since the backup was made. This usually results in much less traffic than replicating the entire database.

The Active Directory Users and Computers tool (ADUC) has been improved to include a new query feature that allows you to write filters for the type of objects you want to view. These queries can be saved and used multiple times. For example, you might want to create a query to show you

all of the users with mailboxes on a specified Exchange server. By creating a query, you can easily pull up a current list with one click of the mouse. ADUC also now supports the following:

- Multi-object selection
- Drag-and-drop capabilities
- The ability to restore permissions back to the defaults
- The ability to view the effective permissions of an object

Group policy management has also been enhanced in Server 2003. The Microsoft Group Policy Management Console (GPMC) makes it easy to troubleshoot and manage group policy. It supports drag-and-drop capabilities, backing up and restoring your group policy objects (GPOs), and copying and importing GPOs. Where the GPMC really shines is in its reporting function. You now have a graphical, easy-to-use interface that, within a few clicks, will show you all of the settings configured in a GPO. You can also determine what a user's effective settings would be if he or she logged on to a certain machine. The only way you could do this in Windows 2000 was to actually log the user on to the machine and run *gpresult* (a command-line tool for viewing effective GPO settings).

In Windows Server 2003, the schema can now be redefined. This allows you to make changes if you incorrectly enter something into the schema. In Windows 2000, you can deactivate schema attributes and classes, but you cannot redefine them. You still need schema admin rights to modify the schema, but now it is more forgiving of mistakes.

The way objects are added to and replicated throughout the directory has been improved as well. The Inter-Site Topology Generator (ISTG) has been improved to support a larger number of sites. Group membership replication is no longer “all or nothing” as it was in Windows 2000. In Windows Server 2003, as members are added to groups, only those members are replicated to your domain controllers and global catalog (GC) servers, rather than the entire group membership list. No more worrying about the universal group replication to your GC servers.

Every domain controller caches credentials provided by GC servers. This allows users to continue to log on if the GC server goes down. It also speeds up logons for sites that do not have a local GC server. No longer is the GC server a single point of failure. In fact, you no longer are required to have one at each site.

Active Directory now supports a new directory partition called the application partition. You can add data to this partition and choose which domain controllers will replicate it. This is useful if you have information you want to replicate to all domain controllers in a certain area, but you do not want to make the information available to all domain controllers in the domain.

Improved File and Print Services

Practically every organization uses file and print services, as sharing files and printers was the original reason for networking computers together. Microsoft has improved the tools used to manage your file system by making the tools run faster than before; this allows users to get their jobs done in less time and requires less downtime from your servers. The Distributed File System (Dfs) and the File Replication Service (FRS) have also been enhanced for Windows Server 2003, and Microsoft has made printing faster and easier to manage.

Enhanced File System Features

Windows 2003 supports WebDAV, which was first introduced in Exchange 2000. It allows remote document sharing. Through standard file system calls, clients can access files stored on Web repositories. In other words, clients think they are making requests to their local file systems, but the requests are actually being fulfilled via Web resources.

Microsoft made it easier to manage disks in Windows Server 2003 by including a command-line interface. From the command line, you can do tasks that were only supported from the GUI in Windows 2000, such as managing partitions and volumes, configuring RAID, and defragmenting your disks. There are also command-line tools for extending basic disk, file system tuning, and shadow copy management.

Disk fragmentation is a problem that commonly plagues file servers. This occurs when data is constantly written to and removed from a drive. Fragmented drives do not perform as well as defragmented drives. Although Windows 2000 (unlike NT) included a disk defragmentation tool, it was notoriously slow. To address this, Microsoft beefed up the defragmenter tool in Windows Server 2003 so that it is much faster than before. In addition, the new tool is not limited to only specific cluster sizes that it can defrag, and it can perform an online defragmentation of the Master Fat Table.

The venerable CHKDSK (pronounced “check disk”) tool, which is used to find errors on Windows volumes, has been revamped as well. Microsoft studies show that Windows Server 2003 runs CHKDSK 20 to 35 percent faster than Windows 2000. However, since Windows 2003 (like Windows 2000) uses NTFS—which is less prone to errors than FAT file systems—you shouldn’t have to run CHKDSK often.

Both the Dfs and the FRS have been improved. Dfs allows you to create a single logical tree view for multiple servers, so that all directories appear to be on the same server. However, they are actually on separate servers. Dfs works hand in hand with Active Directory to determine site locations for clients requesting data, thereby allowing clients to be directed to a server closest to them in physical proximity. FRS is used to replicate Dfs file share data. FRS now allows administrators to configure its replication topology and compress replication traffic.

One of the best file system improvements in Windows 2003 is shadow copies. After you enable shadow copies on the server and install the shadow copy client software on the desktop computer, end users can right-click on a file and view previous versions that were backed up via shadow copies. They can then keep the current version of the file or roll back to an early version. This will remove the burden (to some extent) of simple file restores from your IT staff and allow the users to handle it themselves.

Improved Printing Features

Even though we rely more on electronic communications than ever before, printing is still an important requirement for most companies. One of the more common reasons for small companies to put in a network is for the purpose of sharing printers (a shared Internet connection and e-mail are two other reasons). Microsoft has taken many steps to improve the printing experience in Windows Server 2003. Users who print long documents should notice a performance boost over Windows 2000, because 2003 does a better job of file spooling, print jobs should get to the printer faster.

Microsoft has also made printing easier to manage. Windows Server 2003 has command-line utilities for managing printer configuration, including print queues, print jobs, and driver management. System Monitor has counters for managing print performance.

Installing printers is easy in Windows 2003 because of plug-and-play (PnP) functionality. This allows you to physically connect the printer to the machine and have Windows set it up for you automatically (as long as the printer itself supports PnP). Windows 2003 supports over 3800 new print drivers.

Revised IIS Architecture

Internet Information Services (IIS) is Microsoft's Web server product. IIS 6.0 is included with all versions of Windows Server 2003. With this new version, Microsoft has made great leaps in the area of IIS reliability, availability, management, and security.

IIS 6.0 was designed so a problem with one application won't cause the server or other applications running on the server to crash. It provides health monitoring and disables Web sites and applications that fail too frequently within a defined period of time. IIS 6.0 can stop and restart Web sites and applications based on customized criteria (such as disk, CPU, or memory utilization). IIS 6.0 allows changing the configuration of your Web server without having to restart it. It is the most scalable version of IIS to date, supporting more Web sites on a single server than IIS 5.0. The actual IIS services stop and start much faster than before, helping to decrease Web site downtime.

Management of your Web server is easier in Server 2003, thanks to command-line scripting. The metabase is now stored in a plain-text XML configuration file. This improves backing up, restoring, recovering, troubleshooting, and directly editing the metabase. IIS 6.0 supports ASP .NET, .NET Framework, and a wide variety of languages. Since the .NET Framework doesn't depend on a specific language, almost any programming language will do.

One common complaint about Windows 2000 was that IIS installed by default; thereby creating an instant vulnerability on servers that were never intended to be Web servers. Microsoft recommends that you only install IIS when needed and lock it down so it only offers the services that your organization requires. In Windows Server 2003, IIS is not installed by default and is locked down by default when you do install it. This means that it will only deliver static content, unless you specifically configure it for dynamic content. IIS 6.0 requires an administrator to add necessary dynamic extensions to the Web services extensions list. Until they are added to this list, IIS will not support them; this will stop attackers from calling unsecured dynamic pages.

Enhanced Clustering Technology

A cluster is a group of servers that work together like one computer. Clusters can be used for performance reasons (to balance the load across two or more computers) or for fault tolerant reasons (to provide failover if one computer fails).

Microsoft added clustering support to its OS line in 1997 with Windows NT 4.0 Enterprise Edition. At that time, clustering was not commonly used. Only the really big IT shops could afford to put in clustered solutions because of the cost of the extra servers. Now that hardware has dropped in price, more and more customers are choosing to cluster their mission-critical systems. As Storage Area Networking (SAN) technology becomes more widespread, clusters are becoming fairly easy to set up. Like Windows 2000, Windows 2003 supports two types of clustering: Microsoft Cluster Service (MSCS) and Network Load Balancing (NLB).

Microsoft Cluster Service

MSCS uses two or more physically connected servers, called *nodes*, that communicate with each other constantly. If a node detects that another node is offline, it will take over the services provided by the offline node. However, this happens behind the scenes, and end users are unaware of the process (other than experiencing a small initial delay).

MSCS is traditionally used with mail servers, database servers, and file and print servers. MSCS is supported in Windows Server 2003 Enterprise Edition and Windows Server 2003 Datacenter Edition. Some of the new features of Windows Server 2003 clustering include:

- The support of more nodes in a cluster. Enterprise Edition and Datacenter Edition both support eight nodes.
- Clustering now integrates with Active Directory and creates a computer account for the virtual cluster name.
- Clustered applications can now use Kerberos authentication.

Network Load Balancing

NLB is available in all versions of Windows Server 2003. Unlike MSCS, where only one server offers the services at a time, NLB nodes all offer services at the same time. The NLB cluster is accessed via a virtual name (a name that represents the group of servers as an entity), and whichever server is least busy answers the request (there is a little more to it, but this is good enough for now).

If one server goes offline, there is no transferring of services because all servers offer the services already. When a server goes offline, it is removed from the rotation of servicing requests until it comes back online. NLB is generally used with Web servers, application servers, terminal servers, and streaming media servers. NLB Manager is a new tool in Windows Server 2003 that provides a central point for managing and configuring NLB clusters.

There are many new features for NLB in Server 2003. NLB now supports multiple network interface cards (NICs), allowing a single server to host multiple NLB clusters. You can use virtual clusters to set up different port rules for each cluster IP address, so that each IP address represents a different resource (Web page, application, and so forth). The Internet Group Management Protocol (IGMP) is now supported when NLB is configured in multicast mode. Using IGMP limits cluster traffic on the switch to the ports that have NLB server connected to them. This helps prevent switch flooding. (Switch flooding occurs when every server in an NLB cluster sees every packet addressed to the cluster.) NLB now supports IPSec traffic.

New Networking and Communications Features

Windows Server 2003 adds a number of new networking technologies that enable it to grow with the needs of your business. For example:

- It supports IPv6, which was created to overcome the limited number of addresses in IPv4 (previous versions of NT use IPv4). Windows Server 2003 supports IPv4/IPv6 coexistence through technologies such as Intra-site Automatic Tunnel Addressing Protocol (ISATAP)

and 6to4. Internet and remote access functionality have been enhanced in Windows Server 2003.

- Point-to-Point Protocol over Ethernet (PPPoE) allows making broadband connections to an Internet Service Provider (ISP) without having to load any software.
- Windows can now use IPsec over NAT.
- Remote Authentication Dial-In User Service (RADIUS) has been improved to provide better control over network access and easier troubleshooting of authentication problems.
- Microsoft's implementation of RADIUS, Internet Authentication Service (IAS), can send its logs to a Microsoft SQL Server and it now supports 802.1X authentication and cross-forest authentication.

In Windows 2000, IPsec was not supported through a NAT server. This was a serious drawback for some companies, as it meant they could not VPN through the NAT server using IPsec or the Layer Two Tunneling Protocol (L2TP), which uses IPsec for encryption. This restriction has been removed in Windows Server 2003. Both IPsec connections and L2TP connections using IPsec are supported over NAT when you have a Server 2003 VPN server. This is done using a technology called NAT traversal, or NAT-T. On the client end, the Microsoft L2TP/IPsec VPN client supports NAT-T. It can be downloaded at www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp and can be installed on Windows 98, ME, and NT 4.0 Workstation.

The Internet Connection Firewall (ICF) functions as a personal software-based firewall and provides protection for computers connected to the Internet or unsecured networks. ICF protects LAN, VPN, dial-up, and PPPoE connections by making it easier to secure your server against attacks. With ICF, only the services that you need to offer are exposed. For example, you can use ICF to filter the network connection of your DNS server so that only DNS requests are passed through. ICF is included with the 32-bit versions of the Standard and Enterprise Editions of Windows Server 2003. It is not included with the Web and Datacenter Editions, or with any of the 64-bit versions.

Improved Security

You might have noticed that Microsoft is paying more attention to concerns about security. Many of the new features discussed thus far relate in one way or another to security. One of the key components of Windows Server 2003 security is the Common Language Runtime (CLR) software engine. It reduces the number of security vulnerabilities due to programming mistakes, and makes sure that applications have appropriate permissions to run and that they can run without any errors.

EFS encrypts files that are stored on NTFS-formatted partitions so that it can only be decrypted by the person who encrypted the file, those with whom he or she shares the file, or a designated recovery agent. The sharing of encrypted files is new to Windows XP/Server 2003. In Windows 2000, this was not possible because only the person who encrypted the file had the correct keys to decrypt it. Now, the person who encrypts the file can choose to give other people the ability to decrypt the file as well, and the file encryption key (FEK) is protected by the public key of each additional person who is given authorization. Encrypted files appear just like normal files in Windows Explorer. However, only authorized users can access them. Anyone else will be denied access. EFS now supports encrypting offline files and storing encrypted files in Web folders.

Microsoft provides a single sign-on environment for users via Credential Manager. Credential Manager provides a secure place for users to store their passwords and X.509 certificates. When a resource is accessed, the correct credentials will be pulled from Credential Manager without prompting the user for action. In large complex environments in which you can have three or four user accounts, this is a great benefit. No longer do you have to key in your domain, username, and password each time; you set it up once and then Credential Manager does all of the work.

You can now control which software can run on a machine via software restriction policies. These policies can be applied at the domain, site, OU, or locally. You define a default security level that either allows or disallows software to run via the Group Policy Object Editor Snap-in. Among other things, software restriction policies can be used to prevent viruses and other harmful programs from running on your PC, and can also be used to limit end users to only running the programs needed for their job.

Windows Server 2003 supports the IEEE 802.1X protocols. This standard allows authorization and authentication of users connecting to Ethernet and wireless local area networks (WLANs). Windows Server 2003 supports authentication via Extensible Authentication Protocol (EAP) methods, such as smart cards.

Auto-enrollment and auto-renewal of certificates makes it easier to quickly deploy smart cards. Certificate Services now supports incremental (a.k.a. delta) Certificate Revocation Lists (CRLs), which means that the server can just push down the changes to the client and not have to push the entire CRL every time.

Another new security feature of Windows Server 2003 is Passport Integration. Passport is integrated with Active Directory and supports mapping AD user accounts to Passport accounts. Users can use Passport for a single sign-on to all of the supported systems.

Better Storage Management

In an effort to keep up with the changing times, Microsoft has greatly increased the level of built-in SAN support in Windows Server 2003. The Virtual Disk Service (VDS) provides a unified interface for multivendor storage devices. VDS discovers the storage devices in your network and gives you a single place to manage them.

You can now create and mount a SAN volume from within Windows. In previous versions of Windows, you had to do this from within your SAN application. Also included in Windows 2003, via the driver development kit, is multipathing input/output (MPIO). MPIO allows up to 32 different paths to external storage (for example, SAN).

Microsoft has also put a lot of work into the backup features of Windows Server 2003. The Volume Shadow Copy Services allows you to create a snapshot (or an exact copy) of volumes on your SAN. Clients can then perform shadow copy restores on their own. In other words, clients can look at a list of shadow copies performed on their data and choose to restore their own data from a given snapshot. *NTBackup* also uses shadow copies to make sure that all open files are backed up.

Improved Terminal Services

Terminal Server allows client workstations to function as terminal emulators. Terminal Services client software is installed on the local workstation, allowing it to connect to the terminal server and receive its own desktop session. Multiple clients can run sessions simultaneously. All processing takes place on the server. The client machine is only responsible for managing the keystrokes and mouse

clicks, which are passed over the network to the terminal server via the Remote Desktop Protocol (RDP).

Although RDP is the native protocol for Microsoft Terminal Server and is used with clients running the Windows 2000 Terminal Services client or the XP/2003 Remote Desktop Connection (RDC) client, the Server 2003 terminal server can also be configured to accept connections from Citrix clients using the ICA protocol.

In Windows Server 2003, Remote Administration mode has been renamed to Remote Desktop for Administration and it is installed by default. This works like the Remote Desktop feature in Windows XP. As in Windows 2000, you are still limited to two simultaneous remote desktops at a time. However, there is one improvement: you can now take over the local console session. Terminal Services in Application Server mode is now simply called Terminal Server.

The Windows Server 2003 Terminal Server and Remote Desktop for Administration support more local client devices than in Windows 2000. Now the local client file system, audio output, printers, serial ports, smart cards, and clipboard are supported making it easier for clients to use their local resources while connected to the terminal server. RDP 5.1 is a much more robust client than RDP 5.0 (Windows 2000). It supports display configurations up to 24-bit color at up to 1600x1200 resolution. It also allows customizing the client experience based on available bandwidth. In other words, unnecessary features can be turned off when connecting over a slow link to optimize performance.

Terminal Server is one of the most used features of Windows 2000. It allows users to connect from their local machines and run desktop sessions off of the server. The local workstation at this point is functioning as a “thin client” because all processing is taking place on the server. One common complaint about Terminal Server in Windows 2000 is a lack of support for local resources.

This has been improved in Windows Server 2003. You can now share information easily between your local disk and the server. You no longer must map a drive back to your local workstation. You can print to locally attached printers and use locally attached serial devices. You can redirect the sound from the terminal server to come out of your local speakers. All of these things make using Terminal Server an even more transparent process to the end user.

New Media Services

Microsoft has redesigned Media Services. The version of Media Services in Windows Server 2003 is version 9.0. It is managed via the Windows Media Services Microsoft Management Console (MMC). Media Services provides audio and video content to clients via the Web (Internet or intranet). According to Microsoft, Media Services has been improved in four areas:

- Fast streaming
- Dynamic content
- Extensibility
- Industrial strength

Fast Streaming

Media Services supports fast streaming to ensure the highest quality streaming experience possible even over unreliable networks (for example, wireless networks). Streaming refers to sending video and/or audio in compressed form over the network and playing the data as it arrives. There are four parts that make up fast streaming:

- **Fast start** Supplies instant-on playback without a buffering delay.
- **Fast cache** Supplies always-on playback by streaming to cache as quickly as the network will support and by playing back the stream to the client from cache.
- **Fast recovery** Sends redundant packets to wireless clients to ensure that no data is lost due to connectivity problems.
- **Fast reconnect** Supplies undisturbed playback by restoring connections if the client is disconnected during a broadcast.

Dynamic Content

Media Services supports advertisements and server-side playlists. Advertising support is very flexible, in that ads can be placed anywhere and used as often as wanted in the playlist. You can even use data gathering tools such as cookies to personalize your ads, and all ad data can be logged for further analysis. Server-side playlists are great for clients that don't support client-side playlists. Server-side playlists can contain live data or preexisting content. They allow you to customize the way your content is presented to clients and to make changes quickly and easily without any delay in service.

Extensibility

Microsoft has exposed over 60 Media Services interfaces and their properties, making Media Services a very open platform. Customization can be achieved by using the Microsoft supplied plug-ins or by using the SDK to create your own plug-ins. You can use scripting languages you already know (such as Perl, Visual Basic, Visual Basic Scripting Edition, C, Visual C++, and Microsoft JScript) to customize Media Services.

Industrial Strength

Microsoft boasts that Media Services is the most scalable, reliable, and secure solution on the market today. Media Services in Windows 2003 supports twice as many users per server as Windows 2000. It supports HTTP 1.0/1.1, RTP, RPSP, HTML v3.2, FEC, IPv4/6, IGMPv3, SNMP, WEBM/WMI, SMIL 2.0, SML, SML-DOM, and COM/DCOM. All Media Services plug-ins run in protected memory to guarantee reliability. Many common authorization and authentication methods are supported, such as digital rights management and HTTP Digest. Microsoft provides a Web-based interface, an MMC snap-in interface, and command-line support for administering your media servers.

XML Web Services

XML Web Services are building-block applications that connect together via the Internet. These services provide reusable components that call functions from other applications. It doesn't matter how

these applications were built, the types of devices used, or the OS on the devices used as long as they support XML, because XML is an industry standard. XML Web Services are made available in Windows Server 2003 because of the .NET framework. XML Web Services help provide effective business-to-business (b2b) and business-to-consumer (b2c) solutions.

The Windows Server 2003 Family

The Windows Server 2003 family comes in four different editions: Web Edition, Standard Edition, Enterprise Edition, and Datacenter Edition. It also comes in both 32-bit and 64-bit versions.

Why Four Different Editions?

Although all organizations are different, most would fall into one of three categories: small, medium, and large. The networking needs of organizations in each of these categories are different.

Typically, small organizations are concerned with performance versus cost. They want good performance, but it can't cost a fortune. Large companies want the best performance possible. They aren't as concerned with cost, as long as the product performs as expected. Medium-sized companies fall somewhere in the middle. They sometimes need a little more out of an OS than what a small company will settle for, but they don't need the high-end equipment and features used by very large companies.

Microsoft has tried to create a different edition of Windows for each type of organization, so that all companies can use Windows Server 2003 without overpaying or sacrificing performance. Companies should buy the minimum version of Windows that provides all of the needed features.

Members of the Family

As noted, there are four editions of Windows Server 2003: Web Edition, Standard Edition, Enterprise Edition, and Datacenter Edition. Each edition has its own benefits:

- Web Edition is the least expensive and least functional version. However, if your server is only used for hosting Web pages, then it is a perfect choice.
- Standard Edition is the next step up from Web Edition. Most of the features in Windows Server 2003 are supported in Standard Edition.
- If you need features not provided by Standard Edition or hardware not supported on Standard Edition, then Enterprise Edition would be the next logical choice. Almost every feature in Windows Server 2003 is supported in Enterprise Edition.
- If you need to use Windows System Resource Manager or you need super powerful hardware, then Datacenter Edition is your only choice.

Be sure to pick the version that most closely matches your needs. There are huge differences in price as your work your way up the chain. There is no reason to pay for more than what you need, but you don't want your organization hobbled by limited functionality.

Web Edition

Prior to the release of Windows 2003, if you wanted to have a Windows server function only as a Web server, you would have to buy a copy of Windows 2000 Server and use IIS. This was a waste of money and functionality, because most of the features of Server would never be used. Now there is a version of Windows designed to function exclusively as a Web server, Windows Server 2003 Web Edition. This will save companies a great deal of money and possibly give Microsoft a larger share of the Web server market. There is a difference in price (list price) of around \$700 to \$800 between Web Edition and Standard Edition Server.

Web Edition is meant to host Web pages, Web applications, and XML services. It supports IIS 6.0, ASP.NET, and .NET Framework. Web Edition supports up to two processors and 2GB of RAM. Client access licenses (discussed later in the chapter) are not required when connecting to Web Edition. However, you are only allowed 10 inbound simultaneous SMB connections, to be used for content publishing (this limit does not apply to Web connections). Web Edition allows you to install third-party Web server software such as Apache, Web availability management software such as Microsoft Application Center, and database engine software such as Microsoft SQL Server 2000 Desktop Engine (MSDE).

Web Edition does *not* support the following functions:

- Internet Authentication Services (IAS)
- Microsoft Metadirectory Services
- Domain controller functionality
- Universal Description, Discovery, and Integration Services (UDDI)
- Remote Installation Services

Standard Edition

Windows Server 2003 Standard Edition is the replacement for Windows 2000 Server. It is meant for small to medium-sized businesses and contains most of the features discussed thus far in the book. It is not limited in functionality like Web Edition and it supports up to four CPUs and 4GB of RAM. Standard Edition is a great choice for file and print servers, Web servers, and application servers that don't need to be clustered. It can also function as a domain controller. Microsoft expects Standard Edition to be the most widely used version of Windows Server 2003.

Enterprise Edition

Windows Server 2003 Enterprise Edition is the replacement for Windows 2000 Advanced Server. Enterprise Edition is meant for any sized business, but includes features most often desired by enterprise-level organizations. It provides high performance and reliability. All of the features supported in Standard Edition are supported in Enterprise Edition, as well as support for clustering up to eight nodes. It supports more powerful hardware than Standard Edition, and can use up to eight processors and up to 32GB of memory. There is a 64-bit version of Enterprise Edition for Intel Itanium machines. The 64-bit version supports up to eight processors and up to 64GB of RAM. Enterprise Edition is good for companies that need features or hardware not supported in Standard Edition.

Datacenter Edition

Datacenter Edition is Microsoft's high-end OS. It is meant for companies that need the most reliable and scalable platform available. You cannot buy the Datacenter Edition software and install it yourself; only approved equipment vendors can buy it and they must install it onto approved hardware.

Datacenter Edition contains all of the features found in both Standard Edition and Enterprise Edition; in addition, it adds the Windows System Resource Manager to aid in system management. Datacenter Edition supports up to 32 processors and 64GB of memory in the 32-bit version. The 64-bit version supports up to 64 processors and 512GB of memory. If performance and reliability are at the top of your list (and cost is near the bottom), then Datacenter Edition is an excellent choice.

Licensing Issues

Microsoft based the Windows Server 2003 licensing structure on Windows 2000's structure. However, they have changed some things. This section is not the final word when it comes to Microsoft licensing. This section is meant to serve as a guide on the basics of Windows 2003 licensing. To order licenses, contact your Microsoft Software Advisor. In the United States, call (800) 426-9400, or visit the Microsoft Licensing Program Reseller Web page (<http://shop.microsoft.com/helpdesk/mvlref.asp>). In Canada, call the Microsoft Resource Centre at (877) 568-2495. Outside of the United States and Canada, please review the Worldwide Microsoft Licensing Web site (www.microsoft.com/worldwide).

There are a few rules that you need to know about Microsoft's licensing schemes:

- You have to purchase a product license for every copy of the OS you are going to install.
- Every network connection that is authenticated requires a Windows Client Access License (CAL). Anonymous connections do not require a CAL (for example, anonymous access to a Web page). Windows CALs are not required for Windows 2003 Web Edition, as it is meant to serve Web content only.
- Every Terminal Server session made by a user or device requires a Terminal Server Client Access License (TS CAL). TS CALs are not required for Windows Server 2003 Web Edition, as it is meant to serve Web content only.

The product license allows you to install the OS onto a machine. The CAL allows devices or users to connect to that machine. Microsoft's reasoning behind this is that everyone pays the same price for the base OS, but companies with more connections pay more than companies with fewer connections. This allows them to price according to usage.

There are two licensing modes supported in Windows 2003:

- **Per Server mode** Requires a Windows CAL for each connection. These are assigned to each server and cannot be shared between servers. You are allowed one connection for each CAL assigned to the server. Once the maximum number has been reached, no more connections are allowed.

- **Per Device or Per User mode (formerly called “Per Seat” mode)** Requires that each device or user have its own Windows CAL. These allow the device or user to connect to an unlimited number of servers. With Per Device or Per User mode, the server will not limit the number of connections made as it does in Per Server mode.

Generally, Per Server mode will be most cost effective if you have only one or two servers, and clients that don't always connect at the same time. Per Device or Per User mode will be most cost effective if you have many servers to which your clients need to connect.

Microsoft has two types of CALs, User CALs and Device CALs. User CALs are purchased for every user that makes a connection to a Windows 2003 server. Device CALs are purchased for every machine that makes a connection to a Windows 2003 server. Microsoft recommends that you use either User CALs or Device CALs, but not both at the same time. User CALs are best when you have more machines than users and your users log on to multiple machines to access the servers. Device CALs are better when you have more employees than machines and your users share machines. User CALs and Device CALs are available for both Windows and Terminal Server. Device CALs and User CALs cost the same.

Windows 2000 supported the System Equivalency license for Terminal Server. The System Equivalency license stated that if your client was running the same OS version as the terminal server, then you did not have to buy a Terminal Server CAL (thus, a Windows 2000 Pro machine connecting to a Windows 2000 terminal server did not need a TS CAL). Windows 2003 no longer supports System Equivalency licenses. However, Microsoft does have a Terminal Server licensing transition plan. You can receive a free TS CAL for every copy of Windows XP that you own at the time of the Windows 2003 launch (April 24, 2003). Check out the Microsoft licensing page for more information (www.microsoft.com/licensing).

New to Windows 2003 is the External Connector (EC) license. ECs enable external users to access your server without requiring that you buy CALs for them. External users are people who are not employed by your company. Terminal Server also has an EC license called the Terminal Server External Connector (TS-EC). The EC license is replacing the Internet Connector and TS Internet Connector licenses.

Product Activation

Starting with Windows XP, Microsoft requires OSs to be authorized before a specified number of days pass, after which you won't be able to log on to the OS. Failure to activate only prevents logging on. Services and remote administration are not affected. Windows Server 2003 allows a 30-day grace period for product activation (for retail and OEM products). Companies that use volume licensing do not have to activate their software.

Windows includes an activation wizard. You can activate over the Internet or by phone. One important thing to remember about product activation is that the activation process keeps track of the hardware in your machine. If the hardware changes dramatically, you will have to reactivate your software within three days in order to continue logging on to the server. Microsoft does this to prevent people from purchasing one copy of the OS, activating it, making an image of it, and deploying that image to many more machines.

Installation and Upgrade Issues

Unless your company is buying its first Windows server, you are going to have to decide between upgrading and performing a clean install. Each method has advantages and disadvantages:

- Upgrading preserves many of your existing settings, such as users and groups, permissions and rights, and applications.
- Performing a clean installation can improve the performance of your hard drive, as it will be reformatted during installation. This also gives you a chance to change the partition and volume sizes used on your drives. Clean installs ensure that you don't carry over any existing problems that you might have with your current OS. Some administrators (the authors of this book included) prefer clean installs because they have seen many problems related to OS upgrades in the past. There is something comforting about starting from scratch.

Common Installation Issues

The biggest problems with installing a new OS are hardware and software incompatibilities. It is important to adhere to the recommended hardware specifications for Windows Server 2003. At a minimum, you need the following hardware configuration:

- 133 MHz processor
- 128MB of RAM
- 1.5GB hard drive

Remember that these are the bare minimums on which Windows Server 2003 will run. Obviously, on such old hardware, performance will suffer. Microsoft recommends at least a 550 MHz processor and 256MB of RAM. The more RAM the better.

You should always verify hardware compatibility before you start your installation. There is a system compatibility check you can run from the Windows Server 2003 CD that will check out your hardware for you automatically via the System Compatibility wizard. Even if all of your hardware is supported, you should always update your machine's BIOS to the most recent version.

Common Upgrade Issues

As stated earlier, you should always verify hardware compatibility and BIOS versions. You should always back up your existing system before you start your upgrade. If you have applications on your server, you should read the release notes on application compatibility. These are found in the docs folder on the setup CD (relnotes.htm).

When upgrading servers from NT 4.0 to Windows Server 2003, you must have Service Pack 5 or higher installed. You can perform upgrades from all server versions of NT 4.0 (Server, Enterprise Edition, and Terminal Server Edition). Upgrading Windows 2000 machines to Windows Server 2003 doesn't require any service packs to be installed first. Windows 2000 Server can be upgraded to Windows Server 2003 Standard Edition or Enterprise Edition. However, Windows 2000 Advanced Server can only be upgraded to Windows Server 2003 Enterprise Edition, and Windows 2000

Datacenter Server can only be upgraded to Windows Server 2003 Datacenter Edition. You must have at least 2GB of free hard drive space for all upgrades.

When upgrading Windows NT 4.0 domains to Windows Server 2003 domains, you must first make sure that DNS is installed and properly configured. You don't have to use a Microsoft DNS server, but your implementation of DNS must support service (SRV) records. Optionally, you might want it to support dynamic updates as well. If DNS does not support dynamic updates, you will have to manually create all of the needed SRV records. Before starting the upgrade, you should take one of your BDCs offline. This will allow you to roll back to your existing NT 4.0 environment if you should have problems with the upgrade. Always start your upgrades with the PDC, followed by the BDCs. After upgrading the PDC, you should set your forest functional level to Windows 2003 interim mode.

When upgrading Windows 2000 domains, you must first prepare the forest and the domain for Windows Server 2003 by using the ADPrep tool. You can prepare the forest by running *adprep.exe /forestprep* on the Schema Master, and you can prepare the domain by running *adprep.exe /domainprep* on the Infrastructure Master. ADPrep can only be run from the command line; there isn't an equivalent graphical tool. Unlike when you upgrade from NT 4.0 domains, you do not have to upgrade the PDC (technically the PDC Emulator) first. You can install a new Windows 2003 domain controller into an existing Windows 2000 domain. When upgrading your domain controllers, you need to budget a little growing room for the Active Directory database. The database file (ntds.dit) might grow by up to 10 percent.

Windows Server 2003 Planning Tools and Documentation

Planning is the first step in building a reliable, secure, high-performance and highly available Windows Server 2003-based network. In this section, we'll begin with an overview of network infrastructure planning, introducing you to planning strategies and how to use planning tools.

This section also looks at legal and regulatory considerations, how to calculate total cost of ownership (TCO), and how to plan for future growth. We discuss how to develop a test network environment and how to document the planning and network design process.

Overview of Network Infrastructure Planning

Proper planning of a network infrastructure is essential to ensuring high performance, availability, and overall satisfaction with your network operations. In order to create a viable network design, you'll need an understanding of both the business requirements of your organization and current and emerging networking technologies. Accurate network planning will allow your organization to maximize the efficiency of its computer operations, lower costs, and enhance your overall business processes.

When planning for a new infrastructure or upgrading an existing network, you should take some or all of the following steps:

- Document the business requirements of your client or organization.