Contents

Foreword . . . . . **xxxiii**

Chapter 1 Overview of Windows Server 2003 . . . . . **1**

Introduction 1
Windows XP/Server 2003 1
What's New in Windows Server 2003? 2
New Features 2
New Active Directory Features 3
Improved File and Print Services 4
Revised IIS Architecture 6
Enhanced Clustering Technology 6
New Networking and Communications Features 7
Improved Security 8
Better Storage Management 9
Improved Terminal Services 9
New Media Services 10
XML Web Services 11
The Windows Server 2003 Family 12
Why Four Different Editions? 12
Members of the Family 12
Web Edition 13
Standard Edition 13
Enterprise Edition 13
Datacenter Edition 14
Licensing Issues 14
Product Activation 15
Installation and Upgrade Issues 16
Common Installation Issues 16
Common Upgrade Issues 16
Windows Server 2003 Planning Tools and Documentation 17
Overview of Network Infrastructure Planning 17
Planning Strategies 18
Using Planning Tools 18
Reviewing Legal and Regulatory Considerations 19
Calculating TCO 20
Developing a Windows Server 2003 Test Network Environment 21
Planning the Test Network 22
Exploring the Group Policy Management Console (GMPC) 24
Documenting the Planning and Network Design Process 25
Creating the Planning and Design Document 25

Chapter 2 Using Server Management Tools **27**

Introduction 27
Recognizing Types of Management Tools 28
Administrative Tools Menu 28
Custom MMC Snap-Ins 29
MMC Console Modes 29
Command-Line Utilities 31
Wizards 31
Windows Resource Kit 32

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 Balancing 189
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+I 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 Strategy 243
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 fuctional 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
Transer 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
iisftpdr.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