

Contents

	Foreword	xxxi
	Chapter 1 Active Directory Infrastructure Overview	1
	Introduction	2
1	Introducing Directory Services	2
	Terminology and Concepts	5
	Directory Data Store	5
	Policy-Based Administration	9
	Directory Access Protocol	10
	Naming Scheme	11
	Installing Active Directory to Create a Domain Controller ...	15
1	Understanding How Active Directory Works	19
	Directory Structure Overview	19
	Sites	20
	Domains	21
	Domain Trees	22
	Forests	24
	Organizational Units	25
	Active Directory Components	26
	Logical vs. Physical Components	27
	Domain Controllers	28
	Schema	31
	Global Catalog	31
	Replication Service	32
1	Using Active Directory Administrative Tools	34
	Graphical Administrative Tools/MMCs	35
	Active Directory Users and Computers	38
	Active Directory Domains and Trusts	40
	Active Directory Sites and Services	44
	Command-Line Tools	45

	Cacls	46
	Cmdkey	47
	Csvde	47
	Dcgpofix	49
	Dsadd	49
	Dsget	49
	Dsmode	50
	Dsmove	50
	Ldifde	51
	Ntdsutil	53
	Whoami	54
1	Implementing Active Directory Security and Access Control	55
	Access Control in Active Directory	55
	Role-Based Access Control	60
	Authorization Manager	60
	Active Directory Authentication	61
	Standards and Protocols	62
	Kerberos	62
	X.509 Certificates	63
	LDAP/SSL	63
	PKI	64
1	What's New in Windows Server 2003 Active Directory?	65
	New Features Available on All Windows	
	Server 2003 Computers	68
	New Features Available Only with	
	Windows Server 2003 Domain/Forest Functionality	69
	Domain Controller Renaming Tool	70
	Domain Rename Utility	70
	Forest Trusts	70
	Dynamically Links Auxiliary Classes	70
	Disabling Classes	70
	Replication	70
	Summary of Exam Objectives	72
	Exam Objectives Fast Track	73
	Exam Objectives Frequently Asked Questions	75
	Self Test	76
	Self Test Quick Answer Key	81

Chapter 2 Working with User, Group, and Computer Accounts

83

	Introduction	84
3	Understanding Active Directory Security Principal Accounts	84
	Security Principals and Security Identifiers	85
	Tools to View and Manage Security Identifiers	90
	Naming Conventions and Limitations	92
3	Working with Active Directory User Accounts	99
	Built-In Domain User Accounts	101
	Administrator	102
	Guest	103
	HelpAssistant	104
	SUPPORT_388945a0	104
	InterOrgPerson	104
	Creating User Accounts	105
	Creating Accounts Using	
	Active Directory Users and Computers	105
	Creating Accounts Using the DSADD Command	110
	Managing User Accounts	113
	Personal Information Tabs	115
	Account Settings	118
	Terminal Services Tabs	122
	Security-Related Tabs	126
3	Working with Active Directory Group Accounts	131
	Group Types	131
	Security Groups	132
	Distribution Groups	132
	Group Scopes in Active Directory	133
	Universal	134
	Global	134
	Domain Local	135
	Built-In Group Accounts	135
	Default Groups in Builtin Container	136
	Default Groups in Users Container	138
	Creating Group Accounts	140
	Creating Groups Using Active	
	Directory Users and Computers	141
	Creating Groups Using the DSADD Command	142

	Managing Group Accounts	143
3	Working with Active Directory Computer Accounts	150
	Creating Computer Accounts	150
	Creating Computer Accounts by Adding a Computer to a Domain	151
	Creating Computer Accounts Using Active Directory Users and Computers	152
	Creating Computer Accounts Using the DSADD Command	155
	Managing Computer Accounts	156
3	Managing Multiple Accounts	162
	Implementing User Principal Name Suffixes	162
	Moving Account Objects in Active Directory	164
	Moving Objects with Active Directory Users and Computers	164
	Moving Objects with the DSMOVE Command	165
	Moving Objects with the MOVETREE Command	166
	Troubleshooting Problems with Accounts	168
	Summary of Exam Objectives	170
	Exam Objectives Fast Track	171
	Exam Objectives Frequently Asked Questions	173
	Self Test	174
	Self Test Quick Answer Key	179
	Chapter 3 Creating User and Group Strategies	181
	Introduction	182
	Creating a Password Policy for Domain Users	182
	Creating an Extensive Defense Model	183
	Strong Passwords	184
	System Key Utility	185
	Defining a Password Policy	187
	Applying a Password Policy	187
	Modifying a Password Policy	190
	Applying an Account Lockout Policy	190
	Creating User Authentication Strategies	192
	Need for Authentication	193
	Single Sign-On	194
	Interactive Logon	194
	Network Authentication	195
	Authentication Types	195
	Kerberos	195

Understanding the Kerberos Authentication Process	196
Secure Sockets Layer/Transport Layer Security	197
NT LAN Manager	198
Digest Authentication	199
Passport Authentication	200
Educating Users	202
Planning a Smart Card Authentication Strategy	203
When to Use Smart Cards	205
Implementing Smart Cards	206
PKI and Certificate Authorities	206
Setting Security Permissions	208
Enrollment Stations	209
Enabling Certificate Templates	209
Requesting an Enrollment Agent Certificate	211
Enrolling Users	211
Installing a Smart Card Reader	212
Issuing Smart Card Certificates	213
Assigning Smart Cards	214
Logon Procedures	215
Revoking Smart Cards	215
Planning for Smart Card Support	216
Planning a Security Group Strategy	217
Understanding Group Types and Scopes	218
Security and Distribution Groups	218
Local, Domain Local, Global, and Universal Groups	219
Security Group Best Practices	224
Designing a Group Strategy for a Single Domain Forest ...	225
Designing a Group Strategy for a Multiple Domain Forest	226
Summary of Exam Objectives	230
Exam Objectives Fast Track	232
Exam Objectives Frequently Asked Questions	233
Self Test	235
Self Test Quick Answer Key	241

Chapter 4 Working with Forests and Domains 243

Introduction	244
Understanding Forest and Domain Functionality	244

	The Role of the Forest	246
	New Forestwide Features	247
	The Role of the Domain	254
	New Domainwide Features	256
	Domain Trees	259
	Forest and Domain Functional Levels	259
	Domain Functionality	260
	Forest Functionality	265
1.3.5	Raising the Functional Level of a Domain and Forest	270
	Domain Functional Level	270
	Forest Functional Level	272
	Optimizing Your Strategy for Raising Functional Levels	273
1.3/2.1	Creating the Forest and Domain Structure	275
	Deciding When to Create a New DC	275
	Installing Domain Controllers	276
1.3.1	Creating a Forest Root Domain	278
	Creating a New Domain Tree in an Existing Forest	285
1.3.2	Creating a New Child Domain in an Existing Domain	288
	Creating a New DC in an Existing Domain	293
	Assigning and Transferring Master Roles	300
1.3.3	Using Application Directory Partitions	313
	Establishing Trust Relationships	315
	Direction and Transitivity	315
	Types of Trusts	317
	Restructuring the Forest and Renaming Domains	318
	Domain Rename Limitations	318
	Domain Rename Limitations in a Windows 2000 Forest	319
	Domain Rename Limitations in a Windows Server 2003 Forest	319
	Domain Rename Dependencies	320
	Domain Rename Conditions and Effects	322
	Domain Rename Preliminary Steps	323
	Performing the Rename Procedure	334
	Steps to Take After the Domain Rename Procedure	354
	Implementing DNS in the Active Directory Network Environment	365
	DNS and Active Directory Namespaces	367
	DNS Zones and Active Directory Integration	367
	Configuring DNS Servers for Use with Active Directory	370

	Integrating an Existing Primary DNS Server with Active Directory	370
	Creating the Default DNSApplication Directory Partitions	371
	Using dnscmd to Administer Application Directory Partitions	372
	Securing Your DNS Deployment	373
	Summary of Exam Objectives	374
	Exam Objectives Frequently Asked Questions	376
	Exam Objectives Fast Track	377
	Self Test	379
	Self Test Quick Answer Key	387
	Chapter 5 Working with Trusts and Organizational Units	389
	Introduction	390
1.3.6/ 2.1.1	Working with Active Directory Trusts	390
	Types of Trust Relationships	394
	Default Trusts	395
	Shortcut Trust	395
	Realm Trust	396
	External Trust	396
	Forest Trust	397
	Creating, Verifying, and Removing Trusts	398
	Securing Trusts Using SID Filtering	400
3.3.1/ 3.4.3	Working with Organizational Units	401
	Understanding the Role of Container Objects	402
3.4/ 3.4.1	Creating and Managing Organizational Units	402
	Applying Group Policy to OUs	406
3.4.2	Delegating Control of OUs	407
1.5/1.5.1/ 3.3/3.3.2	Planning an OU Structure and Strategy for Your Organization	408
	Delegation Requirements	409
	Security Group Hierarchy	410
	Summary of Exam Objectives	412
	Exam Objectives Fast Track	413
	Exam Objectives Frequently Asked Questions	414

Self Test	416
Self Test Quick Answer Key	423
Chapter 6 Working with Active Directory Sites	425
Introduction	426
Understanding the Role of Sites	426
Replication	427
Authentication	427
Interactive Logon Authentication	428
Network Authentication	429
Distribution of Services Information	429
Relationship of Sites to Other Active Directory Components	431
Relationship of Sites and Domains	431
Physical vs. Logical Structure of the Network	433
The Relationship of Sites and Subnets	433
1.4/2.2/ Creating Sites and Site Links	434
2.2.3	
Site Planning	434
Criteria for Establishing Separate Sites	435
Creating a Site	436
Renaming a Site	438
Creating Subnets	441
Associating Subnets with Sites	444
1.4.1/2.2.2 Creating Site Links	446
1.4.1/2.2.2 Configuring Site Link Cost	449
2.2/2.2.1/ Understanding Site Replication	452
2.5.1	
Purpose of Replication	452
Types of Replication	453
Intrasite Replication	453
Intersite Replication	454
1.4 Planning, Creating, and Managing the Replication Topology ..	455
Planning Replication Topology	455
Creating a Replication Topology	456
Managing Replication Topology	456
Configuring Replication between Sites	457
Configuring Replication Frequency	457
Configuring Site Link Availability	458

	Configuring Site Link Bridges	458
1.4.2	Configuring Bridgehead Servers	459
2.3	Troubleshooting Replication Failure	459
	Troubleshooting Replication	460
2.3.1	Using Replication Monitor	461
	Using Event Viewer	461
	Using Support Tools	462
2.3.2	Monitoring File Replication Service Replication	463
	Summary of Exam Objectives	465
	Exam Objectives Fast Track	465
	Exam Objectives Frequently Asked Questions	467
	Self Test	468
	Self Test Quick Answer Key	474
	Chapter 7 Working with Domain Controllers	475
	Introduction	476
1.3.4	Planning and Deploying Domain Controllers	476
	Understanding Server Roles	476
	Function of Domain Controllers	480
	Determining the Number of Domain Controllers	481
	Using the Active Directory Installation Wizard	484
	Creating Additional Domain Controllers	494
	Upgrading Domain Controllers	500
	Placing Domain Controllers within Sites	502
	Backing Up Domain Controllers	503
	Restoring Domain Controllers	504
1.2/2.5.2	Managing Operations Masters	505
	Understanding the Operation Masters Roles	505
	Forestwide Roles	506
	Domainwide Roles	507
1.2.1	Transferring and Seizing Operations Master Roles	509
	Transferring FSMOs	510
	Transferring the Schema FSMO	510
	Transferring Domain Naming FSMO	514
	Transferring RID, PDC, or Infrastructure FSMOs	516
1.2.1	Responding to OM Failures	516
	Seizing the PDC Emulator or Infrastructure FSMO	516
	Seizing the RID Master, Domain	

	Naming Master, and Schema Master FSMOs	517
	Summary of Exam Objectives	523
	Exam Objectives Fast Track	524
	Exam Objectives Frequently Asked Questions	526
	Self Test	528
	Self Test Quick Answer Key	537
Chapter 8	Working with Global Catalog Servers and Schema	539
	Introduction	540
	Working with the Global Catalog and GC Servers	540
	Functions of the GC	541
2.1.3	UPN Authentication	541
	Directory Information Search	542
	Universal Group Membership Information	543
	Customizing the GC Using the Schema MMC Snap-In	543
	Creating and Managing GC Servers	545
	Understanding GC Replication	547
	Universal Group Membership	547
	Attributes in GC	547
1.1	Placing GC Servers within Sites	548
1.1.1	Bandwidth and Network Traffic Considerations	549
1.1.2	Universal Group Caching	550
	Troubleshooting GC Issues	552
2.1.2	Working with the Active Directory Schema	551
	Understanding Schema Components	553
	Classes	554
	Attributes	555
	Naming of Schema Objects	559
	Working with the Schema MMC Snap-In	560
	Modifying and Extending the Schema	561
	Deactivating Schema Classes and Attributes	562
	Troubleshooting Schema Issues	563
	Summary of Exam Objectives	564
	Exam Objectives Fast Track	565
	Exam Objectives Frequently Asked Questions	566
	Self Test	567
	Self Test Quick Answer Key	573

Chapter 9 Working with Group Policy in an Active Directory Environment	575
Introduction	576
4/4.2.1 Understanding Group Policy	576
4.3.1	
Terminology and Concepts	577
Local and Non-Local Policies	577
User and Computer Policies	577
Group Policy Objects	580
Scope and Application Order of Policies	580
Group Policy Integration in Active Directory	583
Group Policy Propagation and Replication	583
4/4.1 Planning a Group Policy Strategy	584
4.2.1/4.3.1	
Using RSoP Planning Mode	584
Opening RSoP in Planning Mode	584
Reviewing RSoP Results	587
Strategy for Configuring the User Environment	588
Strategy for Configuring the Computer Environment	590
4/4.2.1 Implementing Group Policy	596
4.3.1	
The Group Policy Object Editor MMC	595
Creating, Configuring, and Managing GPOs	595
Creating and Configuring GPOs	596
Naming GPOs	597
Managing GPOs	598
Configuring Application of Group Policy	600
General	600
Links	601
Security	601
WMI Filter	602
Delegating Administrative Control	604
Verifying Group Policy	604
4/4.2.1 Performing Group Policy Administrative Tasks	608
4.2.2/4.2.3	
4.3.1/4.3.2	
Automatically Enrolling User and Computer Certificates	608

	Redirecting Folders	609
4.1.2/4.1.3	Configuring User and Computer Security Settings	612
4.2/4.2.4		
4.3/4.3.3		
	Computer Configuration	612
	User Configuration	613
	Using Software Restriction Policies	616
	Setting Up Software Restriction Policies	616
	Software Policy Rules	617
	Precedence of Policies	617
	Best Practices	618
4/4.2.1	Applying Group Policy Best Practices	619
4.3.1/5		
4/4.2.1	Troubleshooting Group Policy	621
4.3.1/5.1/		
5.3		
4.1.1	Using RSoP	622
	Using gpresult.exe	623
	Summary of Exam Objectives	628
	Fast Track	629
	Exam Objectives Frequently Asked Questions	631
	Self Test	633
	Self Test Quick Answer Key	639
4.2.1/4.3.1	Chapter 10 Deploying Software via Group Policy	641
	Introduction	642
	Understanding Group Policy Software Installation Terminology	
	and Concepts	642
	Group Policy Software Installation Concepts	644
	Assigning Applications	644
	Publishing Applications	646
	Document Invocation	646
	Application Categories	647
	Group Policy Software Deployment vs. SMS	
	Software Deployment	648
	Group Policy Software Installation Components	648
	Windows Installer Packages (.msi)	649
	Transforms (.mst)	650

	Patches and Updates (.msp)	651
	Application Assignment Scripts (.aas)	652
	Deploying Software to Users	652
	Deploying Software to Computers	653
5.2	Using Group Policy Software Installation to Deploy Applications ...	654
	Preparing for Group Policy Software Installation	654
	Creating Windows Installer Packages	654
	Using .zap Setup Files	656
	Creating Distribution Points	659
	Working with the GPO Editor	660
	Opening or Creating a GPO for Software Deployment	659
	Assigning and Publishing Applications	662
	Configuring Software Installation Properties	664
	The General Tab	665
	The Advanced Tab	665
	The File Extensions Tab	666
	The Categories Tab	666
5.2.1	Upgrading Applications	667
5.2.2	Automatically Configuring Required Updates	668
	Removing Managed Applications	669
	Managing Application Properties	670
	Categorizing Applications	673
	Adding and Removing Modifications for Application Packages	673
	Troubleshooting Software Deployment	675
	Verbose Logging	677
	Software Installation Diagnostics Tool	678
	Summary of Exam Objectives	679
	Exam Objectives Fast Track	679
	Exam Objectives Frequently Asked Questions	681
	Self Test	682
	Self Test Quick Answer Key	688
Chapter 11	Ensuring Active Directory Availability	689
	Introduction	690
	Understanding Active Directory Availability Issues	690
	The Active Directory Database	690
	Data Modification to the Active Directory Database	692
	The Tombstone and Garbage Collection Processes	694

	System State Data	698
	Fault Tolerance and Performance	699
	RAID-1	700
	RAID-5	701
	Performing Active Directory Maintenance Tasks	701
	Defragmenting the Database	702
	Understanding Active Directory Database Fragmentation ...	702
	The Offline Defragmentation Process	703
	Moving the Database or Log Files	707
2.5.3	Monitoring the Database	711
	Using Event Viewer to Monitor Active Directory	711
	Using the Performance Console to Monitor Active Directory	713
	Backing Up and Restoring Active Directory	720
	Backing Up Active Directory	720
	Using the Windows Server 2003 Backup Utility	721
	Backing Up at the Command Line	733
2.4/2.4.1	Restoring Active Directory	733
2.4.2		
	Directory Services Restore Mode	733
	Normal Restore	734
	Authoritative Restore	741
	Primary Restore	743
2.5.3	Troubleshooting Active Directory Availability	745
	Setting Logging Levels for Additional Detail	745
	Using Ntdsutil Command Options	747
	Using the Integrity Command	747
	Using the recover Command	750
	Using the Semantic Database Analysis Command	752
	Using the esentutl Command	756
	Changing the Directory Services Restore Mode Password	758
	Summary of Exam Objectives	759
	Exam Objectives Fast Track	760
	Exam Objectives Frequently Asked Questions	762
	Self Test	764
	Self Test Quick Answer Key	769

Appendix Self Test Questions, Answers, and Explanations	771
Chapter 1: Active Directory Infrastructure Overview	772
Chapter 2: Working with User, Group, and Computer Accounts	781
Chapter 3: Creating User and Group Strategies	789
Chapter 4: Working with Forests and Domains	797
Chapter 5: Working with Trusts and Organizational Units	809
Chapter 6: Working with Active Directory Sites	819
Chapter 7: Working with Domain Controllers	826
Chapter 8: Working with Global Catalog Servers and Schema	840
Chapter 9: Working with Group Policy in an Active Directory Environment	847
Chapter 10: Deploying Software via Group Policy	855
Chapter 11: Ensuring Active Directory Availability	864
Index	873