

Contents at a Glance

<i>Introduction</i>	xvii
Part 1 • Design	1
Chapter 1 • Active Directory Forest Design	3
Chapter 2 • Active Directory Domain Design	19
Chapter 3 • Domain Name System Design	37
Chapter 4 • Sites, Flexible Single Master Operations, and Global Catalog Design ...	51
Chapter 5 • Organizational Unit Design	67
Chapter 6 • Exchange Design Considerations	99
Chapter 7 • Hardware Sizing and Placement	109
Part 2 • Deployment and Migration	119
Chapter 8 • Deployment	121
Chapter 9 • Domain Migration and Consolidation	137
Chapter 10 • NetWare Migration	159
Part 3 • Maintenance and Administration	165
Chapter 11 • Backup and Disaster Recovery	167
Chapter 12 • Optimizing the Active Directory Database	179
Chapter 13 • Troubleshooting Active Directory Replication	195
Chapter 14 • Maintaining DNS	205
Chapter 15 • Troubleshooting the File Replication Service	217
Chapter 16 • Troubleshooting Logon Failures	229

Chapter 17 • Troubleshooting FSMO Roles	243
Chapter 18 • Group Policy	255
Part 4 • Security in Active Directory	273
Chapter 19 • Securing the Base Operating System	275
Chapter 20 • Securing DNS	289
Chapter 21 • Patch Management	301
Chapter 22 • Securing Active Directory	313
Appendix • Scripting Resources	325
<i>Index</i>	327

Contents

Introduction xvii

Part 1 • Design 1

Chapter 1 • Active Directory Forest Design 3

Active Directory Forest Design Criteria	4
Schema	5
Schema Considerations	5
Security Boundary	6
Replication Boundary	7
A Common Global Catalog	8
Kerberos and Trusts	9
Political and Administration Boundary	10
Multiple Forests Pros and Cons	10
Forest Functionality Mode Features in Windows 2003	13
Best Practices for Forest Designs	15
Keeping It Simple: Start with a Single Forest	15
Aiming for the Ideal Design	16
Designing with Change Control Policies in Mind	16
Separating Extranet Applications into Their Own Forest	17
Building a Design Based on the Standard Forest Scenarios	17
Next Up	18

Chapter 2 • Active Directory Domain Design 19

Active Directory Domain Design Criteria	20
Defining Domain Requirements	20
Domain Boundaries	20
Defining Tree Requirements	21
Multiple Domains Pros and Cons	22
DNS Requirements	22
Authentication Options	23
Interforest Trusts	24
Domain Controller Placement	26
Domain Functional Levels	28
Best Practices for Domain Designs	34
Next Up	35

Chapter 3 • Domain Name System Design 37

Tied Together	37
How to Resolve	38
So Many Zone Types	40
How to Name a Zone	44

Internal and External Name Options 45
 Keeping Them Separate 45
 Identical Confusion 45
 Understanding the Current DNS Infrastructure 46
 That Other DNS Server 47
 Propagating the Changes 48
 DNS Design Best Practices 49
 Next Up 49

Chapter 4 • Sites, Flexible Single Master Operations, and Global Catalog Design 51

Determining the Site Topology 51
 Understanding the Current Network Infrastructure 53
 Identifying the Current Network Infrastructure Design 53
 Setting Your Sites to Support the Active Directory Design 55
 Designing Site Links and Site Link Bridges 58
 Site Links 58
 Site Link Bridges 60
 Choosing Global Catalog Placement 61
 Choosing Flexible Single Master Operations Placement 62
 Operations Masters in a Single Domain Forest 63
 Operations Masters Site Placement in a Multiple-Domain Forest 63
 Best Practices for Site Design 65
 Next Up 66

Chapter 5 • Organizational Unit Design 67

Designing OUs for Administrative Control 67
 Understanding the OU Design Options 68
 Understanding OU Design Criteria 73
 Designing OUs for Group Policy 77
 Understanding Company Objectives 80
 Creating a Simple Design 84
 Creating the OU Structure 92
 Best Practices for Organizational Design 96
 Next Up 97

Chapter 6 • Exchange Design Considerations 99

Understanding the Changes 99
 Prepping the Forest 100
 Prepping the Domains 103
 Creating Administrative Groups 105
 Automatic Display Name Generation 105
 Extended Attributes 106
 Best Practices for Design 107
 Next Up 108

Chapter 7 • Hardware Sizing and Placement	109
Determining Domain Controller Specifications and Placement	109
Determining Domain Controller Specifications	110
Choosing Domain Controller Placement	111
Choosing Global Catalog Placement	112
Sizing and Placement Made Simple	113
Choosing Master Operations Placement	116
Best Practices for Hardware Sizing and Placement	118
Next Up	118

Part 2 • Deployment and Migration

Chapter 8 • Deployment	121
Defining Domain Names	121
Identifying the Forest Root Domain	122
Deployment Methods	123
Manual Setup	123
Automatic Setup	124
First Domain Controller	126
Replica Domain Controllers	131
Automating Domain Controller Promotion	134
Best Practices for Deployment	136
Next Up	136

Chapter 9 • Domain Migration and Consolidation	137
Keeping Connected	137
Migration Options	138
ADMT Interface	138
Preparing for Migration	140
ADMT Prerequisites	140
The Rollback Plan	141
Profile Migration	142
Migration Order	142
Maintaining Unique Accounts	143
Verifying Account Status	143
Scripting ADMT	143
Password Migration	144
Migrating from Windows NT 4	145
Migration Strategies	146
Incorporating the Master User Domains	146
Incorporating the Resource Domains	148
Controlling Domain Controller Overrun	149
Emulating a BDC	150
Neutralizing the Emulator	151
Migrating from Windows 2000	151
Prepping the Forest	152

Prepping the Domain154
 Application Issues155
 Upgrade or Reconstruction156
 Other Migration Utilities156
 Best Practices for Domain Migration and Consolidation157
 Next Up157

Chapter 10 • NetWare Migration..... 159

Preparing for Migration159
 A Bird’s Eye View of Migration160
 Application Compatibility161
 Data Migration161
 Mail Migration161
 Mapped Devices162
 Test, Test, Test162
 Train Users162
 Working with Microsoft Directory Synchronization Services163
 Best Practices for NetWare Migration164
 Next Up164

Part 3 • Maintenance and Administration 165

Chapter 11 • Backup and Disaster Recovery 167

Reactive versus Proactive167
 Domain Controller Backup168
 System State Backup168
 Performing a System State Backup168
 Limitations of Windows Backup169
 Restoring Active Directory170
 Directory Services Restore Mode170
 DSRM Password170
 Primary Restore171
 Normal Restore172
 Authoritative Restore172
 The Tombstone173
 Automated System Recovery174
 The ASR Backup175
 The ASR Restore176
 Best Practices for Disaster Recovery176
 Next Up177

Chapter 12 • Optimizing the Active Directory Database 179

Configuring Diagnostic Logging179
 Using ADSI Edit to View Directory Service Partitions181
 Using NTDSUTIL for Active Directory Database Troubleshooting and Repair182
 Committing Transactions to the Database183
 Checking Database Integrity184

Compacting the Database	184
Moving the Database	186
Moving the Log Files	187
Removing Orphaned Objects	187
Maintaining Security Accounts	191
Best Practices for Optimizing AD	192
Next Up	193
Chapter 13 • Troubleshooting Active Directory Replication	195
Replication Overview	195
Determining DNS Problems	196
Verifying Replication	198
Using RepAdmin	200
Using ReplMon	200
Using DCDiag	202
Controlling Replication in Large Organizations	202
Best Practices for Troubleshooting AD Replication	203
Next Up	204
Chapter 14 • Maintaining DNS	205
DNS Resolution Methods	205
Root Domain SRV Record High Availability	208
Active Directory Application Mode	210
Diagnostic Tools	212
Best Practices for Maintaining DNS	215
Next Up	216
Chapter 15 • Troubleshooting the File Replication Service	217
File Replication Service Overview	217
FRS Problems	218
Journal Wrap	218
Morphed Directories	218
Staging Area Problems	219
Parallel Version Vector Joins	219
FRS Troubleshooting Tools	219
Using <i>FRSDIAG.EXE</i>	220
Using Ultrasound	220
Microsoft Operations Manager	225
Common FRS Problem Resolution	226
Best Practices for Troubleshooting FRS	227
Next Up	227
Chapter 16 • Troubleshooting Logon Failures	229
Auditing for Logon Problems	229
<i>Acctinfo.dll</i>	233
Kerberos Logging	234
Native Mode Logon Problems	235

Account Lockout Problems 236
 Remote Access Issues 240
 Are You Being Attacked? 240
 Controlling WAN Communication 240
 Best Practices for Logon and Account Lockout Troubleshooting 241
 Next Up 241

Chapter 17 • Troubleshooting FSMO Roles..... 243

FSMO Roles and Their Importance 243
 Schema Master 244
 Domain Naming Master 244
 Relative Identifier Master 244
 Infrastructure Master 245
 Primary Domain Controller Emulator 246
 Transferring and Seizing FSMO Roles 247
 Identifying the Current Role Holder 247
 Transferring the Role to Another Domain Controller 251
 Seizing the Role on the Standby Domain Controller 252
 Best Practices for Troubleshooting FSMO Roles 253
 Next Up 254

Chapter 18 • Group Policy 255

Troubleshooting Tools 256
 Group Policy Results Tool 256
 Group Policy Verification Tool 258
 Software Installation Diagnostics Tool 259
 Troubleshooting with the Group Policy Management Console 259
 Group Policy Modeling 260
 Group Policy Results 260
 Troubleshooting Methodology 263
 GPO Not Applying 264
 GPO Applying When It Should Not 265
 User Environment Logging 266
 Other Factors to Consider 268
 Handy Dandy Scripts 269
 Best Practices for Group Policy 270
 Next Up 271

Part 4 • Security in Active Directory 273

Chapter 19 • Securing the Base Operating System..... 275

Securing the Domain Controller from a Physical Access Attack 275
 Guarding Against Remote Access Attacks 276
 Domain Controller Auditing Policy Settings 276
 Configuring User Rights Assignments 277
 Domain Controller Security Options 278

Protecting Systems During Installation	281
Use Operating System Best Practices	281
Secure Installation Location	282
Disable 8.3 Auto-Name Generation	282
Securing Well-Known User Accounts	282
Securing Service Accounts	283
Using the Syskey Utility to Secure Password Information	283
Defining Domain Controller Communication with IPSec Filters	284
Modifying the Default Services	285
Best Practices for Securing Domain Controllers	287
Next Up	288
Chapter 20 • Securing DNS	289
Keeping the System Going	289
Limit the Dynamic Updates	290
Monitor for Traffic	290
Separate Namespaces	290
Set Quotas	291
Disable Recursion	293
Use Appropriate Routing	294
Keeping the System Accurate	295
Use IPSec	295
Use Secure DDNS	295
Avoid Cache Poisoning	296
Allow Appropriate Access	296
Lock Down Transfers	298
Best Practices for Securing DNS	299
Next Up	299
Chapter 21 • Patch Management	301
Monitor Security Bulletins and Announcements	301
Determine Systems Affected by Vulnerability	302
Test Patch in a Secure Environment	304
Develop a Deployment Plan	304
Integrate Patch into Live Environment	306
Windows Update	307
Deploying the Patch with Software Update Services	308
Using SMS Server with the SUS Feature Pack to Deploy the Patch	310
Third-Party Solutions	311
Best Practices for Patch Management	312
Next Up	312
Chapter 22 • Securing Active Directory	313
Placement of the Active Directory Database Files	313
Guaranteeing Database Space	314
Auditing Domain Controllers	314
Maintaining the Service Account Administrators	321

Creating a Baseline	322
Using Secure Administrative Methods	322
Secondary Logon	322
Trustworthy Personnel	322
Two-Person Authentication	323
Controlling Cached Credentials	323
Best Practices for Securing Active Directory	323
Next Up	324
Appendix • Scripting Resources	325
From Microsoft	325
From Third-Party Vendors	326
<i>Index</i>	327