



Microsoft®



CD-ROM
included

Building Enterprise Active Directory™ Services

Notes from the Field

Real-world
information for
planning and implementing
Active Directory services

**Best Practices
from Microsoft
Consulting
Services**

Suranaree University of Technology



31051000653622

IT Professional

Contents

Introduction	xiii
What's in This Book	xiv
Part I: Setting the Foundation	xiv
Part II: Migration and Integration Scenarios	xv
Part III: Administration and Security	xv
Icons That Highlight Text	xvi
What's on the Companion CD-ROM	xvi
How To Use the Companion CD-ROM	xviii
System Requirements	xviii
A Well-Deserved "Thank You"	xviii
Some Important Business	xviii
Contributors	xix

Part 1 Setting the Foundation

Chapter 1 Windows 2000 Active Directory Design	3
Overall Design Process at Woodgrove Bank	5
Stages and Deliverables	5
Teams	6
High-Level Design Goals	7
Assessment of the Current Windows NT 4.0 Environment	8
Current Network Architecture	8
Current Domestic Windows NT 4.0 Domain Architecture	9
Current International Windows NT 4.0 Domain Architecture	10
Windows 2000 Design	12
Business Requirements for Active Directory	12
Woodgrove Bank Active Directory Design	12
Single Domestic and Separate International Domains	13
Next Generation INTL Design	45
Conclusion	47

Chapter 2 Compaq's Windows 2000 Site Topology Design	49
Fundamentals of Active Directory Replication	51
Domain Controllers	51
Triggering Replication	52
Update Types	52
Naming Contexts	53
Sites	54
Bridgehead Server	55
Replication Transports	56
Knowledge Consistency Checker	57
Connection Objects	57
Global Catalog Replication	58
Compaq's Corporate Namespace	59
Network Infrastructure	61
GlobalNet	61
Addressing Considerations	62
Legacy Networks	64
Site Topology Design	64
Intra-Site vs. Inter-Site Replication	66
Creating Replication Topologies	67
Site Topology	67
Server Location	72
Conclusion	77
Chapter 3 Active Directory Database Sizing	79
Active Directory Database Architecture and Components	81
General Structure	81
Database Structure	82
Changes to the Database	83
Garbage Collection	85

Active Directory Database Sizing Tests—Single Objects	86
Calculating Growth and Object Sizes	87
Single Object Type Loads	87
User Objects	87
Adding Attributes	89
Organizational Units	90
Groups	91
Contacts	96
Storing Public Key Certificates in the Active Directory	97
Printers and Volumes	98
Storing BLOBS in the Active Directory	99
Active Directory Database Sizing Tests—Sample Company	100
Sample Company with Minimum Properties	101
Sample Company with Custom Attributes	101
Access Control Entries	102
Reclaiming Space in the Database	104
Summary of Database Sizing Tests	107
Active Directory Database Sizing Tests—Global Catalog Servers	107
Global Catalog Servers with Sample Company	108
Global Catalog Servers and Sample Company with Universal Groups	109
Global Catalog Sizing with Individual Objects	110
Global Catalog Summary	112
Adding Microsoft Exchange 2000	113
Extending the Schema with Exchange 2000	113
Adding Mailboxes to Users	114
Mail-Enabling Groups	117
Mail-Enabling Contacts	118
Sample Company with Exchange 2000	120
Summary Active Directory Objects with and without Exchange 2000	122
Conclusion	123
Chapter 4 Active Directory Replication Traffic Analysis	125
Why Measure Replication Traffic?	127
Types of Replication Traffic	128
Replication Scenarios	130
How To Measure Replication Traffic	131

Intra-Site Replication	131
RepAdmin	133
MMC Forced Replication	134
Summary of Replication Options	135
Modeling Replication Traffic	136
Global Catalog and Intra-Domain vs. Inter-Domain Replication	137
Single Attribute Changes	138
Intra-Site Domain Object Replication	142
Intra-Site GC Replication	146
Inter-Site Replication	151
Inter-Site Domain Replication	152
Adding User Attributes	157
Replication of Password Changes	160
Changing Group Memberships	161
Administrative Operations	162
Global Catalog Server Replication	171
Adding User Objects	172
Replicating Groups	174
Printers and Volumes	177
Tuning SMTP Replication	178
Inter-Site Traffic Calculation Tables	181
Slow Link Replication	181
Conclusion	183
Chapter 5 Active Directory Client Network Traffic	185
Windows NT 4 Client Logon Traffic	187
Overview	187
Workstation Boot Process	189
User Logon	192
Windows 2000 Professional Logon Traffic to Active Directory	195
Test Harness Setup	197
Effect of Group Membership on Logon Traffic	198
Effect of Group Policy on Logon Traffic	200
IntelliMirror Technology	207
NetBIOS Traffic	212
Detailed Description of the Windows 2000 Professional Workstation Logon Traffic	213

LDAP Concepts, Operations, Traffic, and Capacity Planning for Active Directory	213
Informational Model	214
Naming Model	216
Functional Model	217
Additional Concepts	218
Active Directory LDAP Traffic Analysis	231
Test Environment	231
Analyzing Interrogation	246
Analyzing Update	254
What Is Not Covered	261
Conclusion	262

Part 2 Migration and Integration Scenarios

Chapter 6 Domain Migration and Consolidation	265
The Environment	267
The Windows NT 4.0 Domain Model	267
Proposed Active Directory Model	268
Determining the Migration Scenario	269
Creating the Active Directory Infrastructure	270
Root-Level NWT.INT Domain	270
Second-Level NA.NWT.INT Domain	270
Migrating the UK Domain (In-Place Upgrade)	271
Why In-Place?	271
Order of Upgrade	272
The Process	272
Maintaining Interoperability	275
Consolidating the North American Domains	275
Why Consolidate?	275
The Active Directory Migration Tool	276
Order of Migrations	276

The Migration Process	276
Devise and Test a Back-Out Plan	276
Establish and Apply a Duplicate Names Policy	277
Establish and Apply a Uniqueness Policy	277
Identify and Remove Obsolete Global and Local Groups	277
Establish Necessary Trust Relationships	277
Clone Global Groups to the Windows 2000 Domain	278
Clone Shared Local Groups to the Windows 2000 Domain	280
Clone User Accounts to the Windows 2000 Domain	282
Moving Computer Accounts to the Windows 2000 Domain	283
Migrate a Pilot Group to the Windows 2000 Domain	283
Migrate Remaining Domain Members to the Windows 2000 Domain	284
Interoperability During Migration	284
Decommissioning the Source Domains	285
Using ClonePrinciple, Netdom, and MoveTree	286
Future Plans	287
Resource Domain NWTRDUK	287
North America Resource Domains	287
Branch Offices	287
Conclusion	287
Chapter 7 Integrating Active Directory with a Unix-Based DNS Environment	289
Before You Begin	291
Infrastructure and DNS Strategy	291
Why a Pure Unix DNS Solution?	293
DNS Requirements for Active Directory	293
Comparing Bind and Windows 2000 DNS	294
Active Directory Storage and Replication Integration	294
Secure Dynamic Update	294
Caching Resolver	295
DNS Snap-In	295
WINS Integration	295
UTF-8 (Unicode) Character Support	296
Aging/Scavenging Support	296
DNSCMD Command Line Utility	296
Upgrade Options for a Unix DNS Environment	296

Configuring a Pure Unix DNS Environment	298
Unix Server Configuration	298
Windows 2000 Server Configuration	303
Windows 2000 DHCP Server Configuration	304
Down-Level DHCP Servers	305
Windows 2000 Clients	306
Down-Level Clients	307
Additional Considerations	307
Bind 4.x and 8.1.2 Servers	307
Windows 2000 Domain Controllers and DHCP Servers	308
Conclusion	308
Chapter 8 Integrating Active Directory with Exchange Server	309
Upgrade Strategy Overview	311
Profile of All-Terrain Trucking	311
Project Background	312
Upgrading Windows NT 4.0 Domains to Windows 2000	317
Summary of ACCOUNTS Domain Upgrade	318
Summary of EXCHANGE Resource Domain Upgrade	321
Collapsing Resource Domains	322
Directory Replication and Synchronization	328
The Active Directory Connector	329
Using Connection Agreements to Establish Relationships	330
Replication	331
Synchronization	331
Installing and Configuring the Active Directory Connector	332
Step 1: Examine Windows NT Domain Structure and Exchange Server Site Topology	333
Step 2: Determine Which Directory Service Will Manage Object Identity	334
Step 3: Perform Active Directory Schema Modifications	335
Step 4: Define Objects for Directory Synchronization	335
Step 5: Map Exchange Server Sites/Containers to Active Directory Domains/OUs	336
Step 6: Determine the Attribute Map Between Active Directory and Exchange Server	337
Step 7: Set Up the Active Directory Connectors	339
Step 8: Create Connection Agreements To Populate Active Directory from Exchange	340
Step 9: Determine a Schedule for Directory Replication and Synchronization	341

Step 10: Create Connection Agreements for Maintaining Directory Synchronization	343
Step 11: Secure Directory Services To Prevent Collisions and Maintain Identity	346
Summary of Active Directory Connector	349
Planning for Exchange 2000	350
Exchange 2000 Uses the Active Directory	350
Exchange 2000 ADC Update	350
Before Upgrading to Exchange 2000	350
Conclusion	351
Lessons Learned	352
Chapter 9 Active Directory and Novell NetWare NDS	355
Network Directory Overview	357
The Schema: Objects, Classes, and Attributes	358
Hierarchy and Containers	359
Security and Delegation	360
Replication and Synchronization	360
Partitioning	361
Comparing NDS and Active Directory	362
Container Objects	362
Catalogs	366
Replication Overview	368
Multi-Master Updates	368
Authentication	369
Security and Inheritance	370
Internet Standards	370
Designing Solutions in Active Directory and NDS	373
Rules for Designing a Directory	373
About Northwind	373
The Design Process	374
Synchronization Between Active Directory and NDS	384
The Need for Synchronization	384
Publishers, Subscribers, and Sessions	385
Configuring MSDSS	385
Synchronization Types	389
Management	389
Conclusion	389

Part 3 Administration and Security

Chapter 10 Scripting the Active Directory	393
Basics	395
What Is ADSI?	395
Windows Scripting Host	396
Active Server Pages	397
HTML Applications	398
Using Visual Basic for Applications in Office 2000	398
ADSI Basics	398
Architecture	398
Connecting to the Active Directory	399
Reading an Object	400
Updating an Object	400
Enumerating a Container	401
Searching	401
Managing Domain Information	402
Extracting Computer Information	402
Trust Relationships	404
Creating User Accounts	405
Creating Groups	406
Managing Enterprise Configuration Information	409
Partitions	409
Listing Sites	410
Creating Sites	412
Listing Subnets	413
Creating Subnets	413
Listing Domain Controllers	414
Site Links	417
Replication Connections	418
FSMO	420
IADSTools Examples	421
WMI	423
Conclusion	428

Chapter 11 Delegating Tree/Forest Operations	429
Delegating: Reasons and Consequences	431
Background	432
Central Office	432
Root Domain Management	432
Schema Management	433
Child Domain Pre-Creation Procedures	434
Site Management	438
Site Link Management	439
DNS Root Management	440
Other Windows 2000 Services	441
Security	441
Conclusion	444
Chapter 12 Building a Windows 2000 Public Key Infrastructure	445
Introduction to Public Key Infrastructure	447
Encryption	447
Digital Signatures	448
Digital Certificates	448
Trust and Certificate Authorities	449
Core Components of the Microsoft PKI	450
Why Use the Microsoft PKI?	451
Planning and Designing a Public Key Infrastructure	452
Case Study: Trey Research	452
Analyzing Business Requirements	452
Defining a PKI Topology	456
Specifications of the Individual CAs	461
Defining Public Key Policy Settings (GPO)	469
Defining the Security Policy, Certificate Policies, and the Certificate Practice Statement	471
PKI Maintenance and Administration	472
Conclusion	474
Index	475