


Contents

	Preface	xxv
Understand What Is in a Directory Service	Part I: Getting Started	1
	Chapter 1 Introduction to Active Directory	3
	Introduction	4
	Introduction to Directory Services	4
	Directory Enabled Networks	5
	History of the Directory Service	6
	What Is in a Directory Service?	11
	The Directory Database	13
	Directory Service Domino Effect	15
	Introduction to Active Directory	15
	.NET	16
	Protocol Interoperability	17
	Single Point of Administration	18
	Active Directory Architecture	20
	Namespace	23
	Forests	24
	Scope	24
	Distinguished Name	25
	User Principle Name	26
	Partitions	27
	Global Catalog	28
	Object	29
	Container	29
	Domains	30
	Domain Trees	30

Viewing Trust Relationships	30
Viewing the Namespace	31
Sites	32
Architecture	33
Data Model	33
Schema	33
Security Model	34
Administration Model	35
Summary	36
Solutions Fast Track	37
Frequently Asked Questions	39

Chapter 2 Assessing Your Environment 41

Estimate Project Costs

- **Labor** How many people will be required to work on the project?
- **Capital** What server equipment will need to be purchased?
- **Real estate** Will you require more space for servers?
- **Training** Will your administrators need to be trained on the new system?
- **Ongoing costs** What are the costs of a maintenance contract for the hardware?

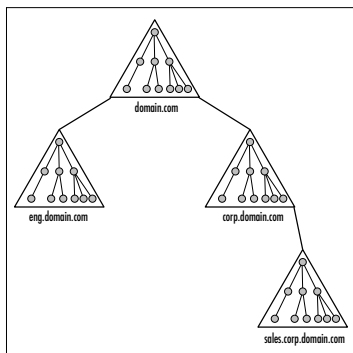
Introduction	42
Defining Your Business Objectives	43
Matching Business Objectives to Technology	45
Business Objectives That Active Directory Will Meet	47
Costs and Benefits	50
Project Costs	50
Benefits	51
Assessing Your Current Environment	52
Network Infrastructure	55
Servers	56
Desktops	57
Peripherals and Mobile Devices	57
Locations	58
Gathering Information for Your Active Directory	
Planning and Design	59
Objects and OUs	59
Organizational and Network Infrastructures That Impact Active Directory Planning and Design	59
Planning for Your Implementation	61
Project Timeline	61
Setting Milestones	63
Setting a Budget	63

Communications	64
Gap Analysis of Business Objectives and Current Environment	65
Risk Analysis	66
Summary	68
Solutions Fast Track	68
Frequently Asked Questions	70

Chapter 3 Active Directory for Windows 2000 JumpStart Tutorial 73

Introduction	74
What Active Directory Is, and Why You Need to Know About It	74
Demote a DC	75
Policy-Based Administration	76
Decentralized Administration	76
Improved Security	77
Important Features	77
Scalability of Forests, Domains, Organizational Units, and Sites	78
Extensibility of the Schema	80
Multi-Master Domain Controllers	82
Intellimirror	82
Kerberos Trusts	84
Use of Standard Protocols	85
Accessibility of Resources	86
Industries and Companies Affected by Windows 2000	87
Technology Vendors and Partners	88
Competitors	88
Customers	89
And... Microsoft Itself	90
Advantages and Disadvantages of Active Directory	90
Advantages with Active Directory	90
Problems with Active Directory	91

Learn about Domain and Domain Trees



Summary	93
Solutions Fast Track	93
Frequently Asked Questions	95

Part II: Designing the Active Directory 97

Chapter 4 DNS and Naming Strategies 99

Answer Your Questions about DNS



Q: Can we use a DNS server other than Windows 2000 DNS?

A: Yes, but it must be able to support SRV RRs. Even if you have a Windows NT 4.0 DNS server, you will not be able to use it because it doesn't support SRV RRs. However, a BIND 8.1.2.1 server can be used because it does support SRV RRs.

Q: Our company uses a DNS server that does not support SRV resource records (RRs). Can we use it when we implement Active Directory?

A: No. Active Directory relies on SRV RRs in order to locate domain controllers (DCs). All DNS servers for the namespaces that Active Directory encompasses must also support the SRV RRs.

Introduction	100
What Is DNS?	101
How DNS Zones Function	104
Active Directory's Integration with DNS	106
How Active Directory Uses DNS	108
Dynamic DNS	112
Planning Active Directory and DNS	113
Forest Plan	114
Domain and DNS Strategy	116
DNS Sizing	117
Domain Divisions	117
Requirements	118
Root Domain	119
About Domains	120
DNS Servers	120
Organizational Units	121
Site Topology	122
Naming Conventions	123
Defining DNS Names	125
Defining DNS Zones	127
Naming Conventions for Active Directory	127
Migrating an Existing Exchange Server	
Design	129
Migrating an Existing Novell	
Directory Services Design	129
Summary	131
Solutions Fast Track	132
Frequently Asked Questions	133

Design the Active Directory

When you design an Active Directory, there are four elements that must be planned:

- Forest Plan
- Domain/DNS Strategy
- Organizational Unit (OU) Structure
- Site Topology

Understand the Components of the Active Directory Sites and Services Console Found in Administrative Tools



Chapter 5 Designing the Basic Structure	135
Introduction	136
Case Studies	136
About Tekkietech.com	136
About Insurance, Inc.	138
Designing a Forest	140
Tekkietech.com	141
Insurance, Inc.	142
Designing a Domain Tree	143
Tekkietech.com	145
Insurance, Inc.	146
Designing an Organizational Unit Structure	148
Tekkietech.com	148
Insurance, Inc.	150
Designing a Site Topology	150
Tekkietech.com	152
Insurance, Inc.	152
Using OUs for Delegating Administration	154
OU Objects in Active Directory	155
Group Policy and OUs	155
Delegating Administration	155
Summary	160
Solutions Fast Track	161
Frequently Asked Questions	163
Chapter 6 Designing a Site Structure	165
Introduction	166
The Function of Sites in Active Directory	167
Default-First-Site-Name	170
Replicated Active Directory Components	171
Domain Partitions	171
Global Catalog	171
Schema and Configuration Containers	173
Site Replication Components	174
Site Objects	174
Knowledge Consistency Checker	174

Connection Objects	175
Site Links	176
Site Link Bridges	177
Replication Protocols	179
Replication in Active Directory	180
Replication Topology	181
Planning a Site Structure	187
Placing Domain Controllers	190
Where to Place Global Catalog Servers	191
Summary	192
Solutions Fast Track	193
Frequently Asked Questions	194

Learn the Goals of Placing Servers

One of the essentials of site design is to place servers in the various locations. When placing servers, there are some simple goals:

- Ensure that users can log on to and query Active Directory.
- Ensure that servers can locate other domain controllers.
- Manage traffic generated by Active Directory.

Chapter 7 Designing: A Case Study 197

Introduction	198
Case Study Overview	198
Assessing a Corporate Network	200
Determining the Business Objectives	200
Kings Vineyard’s Business Objectives	201
Current Environment	203
Network Infrastructure	204
Servers	206
Desktops and End-Users	207
Designing the Forests	208
Determining Domain and Tree Structure	210
Planning the OU Structure	214
Administrative Structure	214
Hidden OUs	215
Group Policies	217
Inheritance	222
Establishing the Initial Sites	222
Site Links	223
Placing Servers	224
Domain Controllers	224
Global Catalog Servers	226
DNS Servers	226

Summary	227
Solutions Fast Track	227
Frequently Asked Questions	229

Part III: Installing Active Directory 231

Chapter 8 Migrating from NT 3.51 or NT 4 to Active Directory 233

Introduction	234
Server Migration Strategies	235
Primary Domain Controllers	243
Changes Required When Upgrading a Domain Controller	245
Backup Domain Controllers	246
Member Servers	248
Promoting Member Servers with Dcpromo	248
Upgrading with the Windows 2000 Setup Wizard	249
Installing Active Directory Services	251
Interim Mixed Domains	255
Mixed Mode	255
Native Mode	256
Migrating Components	257
Using Organizational Units to Create a Hierarchical Structure	258
User Accounts	260
ClonePrincipal	261
Active Directory Migration Tool	261
Machine Accounts	262
Nested Groups	263
Global Groups	264
Delegating Administrative Authority	264
Insert into the Replication Topology	265
Upgrading Clients to Windows 2000 Professional	266

Decide Whether to Upgrade Servers or Clients First



This decision is in line with long-standing networking best practices when deploying new networks:

1. Establish the network infrastructure first.
2. Establish security and servers next.
3. Establish workstations last.

Learn the Three Basic Steps for the Windows 2000 Active Directory Domain Installation

1. Run the Windows 2000 Server installation command. (You have the option of running WINNT from a DOS prompt, booting directly into the installation from the CD-ROM, or running WINNT32 from a 32-bit Windows operating system.)
2. Configure DNS (Domain Name System) as a client to another DNS server or as a service on the Windows 2000 Server.
3. Run the Active Directory Installation Wizard.

Summary	269
Solutions Fast Track	271
Frequently Asked Questions	273

Chapter 9 Implementing a Domain 275

Introduction	276
Installing DNS	277
Verifying Compatibility	277
Windows 2000 DNS Installation	279
Delegating a Subdomain	279
Configuring DNS	281
About Zones	282
Service Resource Record Registration	284
Installing Domains in Active Directory	284
Active Directory Sizer Tool	285
The First Domain Controller	285
Active Directory Wizard	289
Integrating DNS into Active Directory	298
Active Directory Integrated Zones	299
Managing Objects in Active Directory	300
Creating Organizational Units	300
Managing User Accounts	301
Managing Groups	303
Nesting Groups	305
Managing Computers	306
Common Object Management	308
Role-Based Administration	308
Microsoft Management Console	308
Administrative Roles	309
Summary	311
Solutions Fast Track	312
Frequently Asked Questions	314

Chapter 10 Building Trees and Forests 317

Introduction	318
Understanding the Characteristics of an Active Directory Forest	319

Learn the Five Major Command Line Programs

- NETDOM BDC
- NETDOM MASTER
- NETDOM MEMBER
- NETDOM QUERY
- NETDOM RESOURCE

Common Schema	320
Common Configuration	320
Global Catalog	320
Contiguous Namespace	322
Trust Relationships	323
Transitive Bidirectional Trust	323
Trusts That Cross Forests	324
Trust Utilities	325
Implementing the Forest Structure	329
The Domain Tree Structure	331
Adding a Child Domain	333
Right-Sizing the Active Directory Storage Space	334
Managing the Forest	338
Summary	342
Solutions Fast Track	343
Frequently Asked Questions	345

Find Complete Coverage of Replication Utilities

- REPLMON is a Windows 2000 Resource Kit utility that you can use to monitor replication traffic.
- REPADMIN is a command-line utility that you use to diagnose problems with replication.
- Although DSASTAT is not geared specifically towards replication, it can help diagnose replication problems that are based in naming context issues.

Chapter 11 Implementing Sites	347
Introduction	348
Creating Site Components	348
Creating Sites	348
Creating Connection Objects	350
Creating IP Subnets	351
Creating Site Links	352
Creating Site Link Bridges	355
The Knowledge Consistency Checker	356
Implementing a Site Structure in Active Directory	356
Replication Utilities	361
Replication Monitor	361
Replication Administrator	362
DSASTAT	362
Understanding Time Synchronization	362
Summary	364
Solutions Fast Track	365
Frequently Asked Questions	367

Case Study

In this chapter, you will be provided with an exemplary organization's Active Directory design, and then will walk through its implementation.

Chapter 12 Implementing Active Directory: A Case Study 369

Introduction	370
Case Study Overview	370
Forest Plan	370
DNS and Domain Plan	370
Organizational Units	373
Site Topology Plan	373
Implementing DNS	375
Implementing the First Domain Controller	377
Migrating	377
Upgrading	378
Adding New Domains	379
Creating an Explicit Trust	381
Establishing the OUs	382
Moving Upgraded Users	382
Creating New Users	383
Adding Computer Objects	383
Setting Up Sites	384
Summary	386
Solutions Fast Track	386
Frequently Asked Questions	388

Part IV: Migrating Active Directory 391

Chapter 13 Intellimirror 393

Introduction	394
What Are Group Policies?	394
How Group Policies Are Applied	397
Refresh Interval	397
Blocking and Enforcing	398
Group Policy Information Storage and Settings	400
Administrative Templates	400
Registry.pol	402
Group Policy Settings	402
Computer Configuration	403
User Configuration	403
Designing a Group Policy Strategy	405

Group Policy in WAN Environments	406
Implementing a Group Policy Strategy	408
Configuring Group Policy Objects	409
Link a Group Policy Object to a Container	412
Adding Scripts	413
Deploying Applications with Group Policies	416
Folder Redirection	420
Keeping Groups from Growing Over Time	423
Troubleshooting Group Policies	424
Policy that Does Not Execute	424
A Policy that Executes in the Wrong	
Way	425
Logging On Takes a Long Time	426
Understanding Security	426
Groups	427
Domain Security Console	429
Account Policies	430
Local Policies	434
Event Log	434
Restricted Groups	434
System Services	435
Registry	435
File System	435
Public Key Policies	436
IP Security Policies on Active Directory	436
Security Templates	436
Object Protection	436
Access Control Lists	436
Access Control Entries	437
Security Descriptor	438
Security Identifier	439
Security Model	439
Kerberos	440
Public Key Infrastructure	440
Smart Cards	441
IP Security	441
Secondary Logons	441

Learn about the Four Containers to which Group Policies Might Be Applied

- Local Group Policy
- Site Group Policy
- Domain Group Policy
- Organizational Unit (OU) Group Policy

Summary	443
Solutions Fast Track	444
Frequently Asked Questions	446

Chapter 14 Publishing 449

Four ADSI objects are capable of extending a directory service schema. They are called schema management ADSI objects:



- **Schema container**
Contains the target directory service schema.
- **Class container**
Defines object classes for the target directory service.
- **Property object**
Defines object attributes for the target directory service.
- **Syntax object** Further defines the syntax used for a property object.

Introduction	450
Publishing Resources	450
Sharing Folders	451
Publishing a Folder in Active Directory	452
Browsing and Querying for Shared Folders	454
Overview of Dfs and EFS	457
Dfs	457
EFS	458
Publishing a Printer in Active Directory	459
Interfacing with Active Directory	460
ADSI	460
RPC	462
Windows Sockets	463
DCOM	463
Exchange Server 5.5 Active Directory Connector	463
Exchange Server 2000	465
Summary	469
Solutions Fast Track	469
Frequently Asked Questions	471

Chapter 15 Modifying the Schema 473

Introduction	474
About Objects and Attributes	474
Planning Schema Modifications	475
Why Modify the Schema?	475
When to Modify the Schema	476
Who Should Modify the Schema?	476
Schema Management Console	478
Flexible Single Master Operation	479
How to Modify the Schema	481
Class	481

Attributes	488
System Checks after Schema Modification	490
Schema Container	491
The Cache	491
Schema Utilities	492
Querying Active Directory	494
Display Specifiers	494
Summary	496
Solutions Fast Track	497
Frequently Asked Questions	499

NOTE

You can reduce some administrative headaches by setting up a refresh for users' profiles. If you delete the user profile cache, a user must authenticate to the network and load a new profile. Be selective when choosing users to refresh profiles on, however. Authenticating and downloading profiles may not be desired for remote users, especially if they have large profiles to load or are often traveling.

Chapter 16 Using Active Directory: A Case Study 501

Introduction	502
Case Study Overview	502
Planning the Group Policy Solution	504
Creating New OUs	505
Deciding Group Policy Application	506
Determining What Group Policies Are Needed	507
Implementing the Group Policy	507
Computer Node	508
User Node	509
Creating the Group Policy for an OU	513
Creating Logon/Logoff Scripts	514
Summary	516
Solutions Fast Track	516
Frequently Asked Questions	518

Part V: Integrating with Active Directory 521

Chapter 17 Plugging into Active Directory 523

Introduction	524
Microsoft's Metadirectory	524
MMS Architecture	528
Obtaining MMS	529

Microsoft's Active Directory Deployment Tools	529
Mission Critical's Active Directory Migration Tool	530
Deploying Active Directory-Enabled Clients	530
Best Practices	530
Deploying DSClient	531
Quest's FastLane Technologies	532
FastLane Reporter	533
FastLane Administrator	534
FastLane Migrator	535
FastLane Developer	537
FastLane Consolidator	537
Cisco	537
CNS/AD	538
What CNS/AD Does	540
Other Applications	541
SAP	542
Mobile Information Server	542
SQL Server 2000	543
Summary	544
Solutions Fast Track	545
Frequently Asked Questions	547

Recovering a Failed Domain Controller

When a DC fails, there is typically more to be restored than just files and folders. There are two issues involved:

- Transactions might not have been written to disk, but were written to log files for Active Directory.
- Data in the Active Directory databases on other DCs might have had additional changes since the failure.

Chapter 18 Disaster Recovery for Active Directory 549

Introduction	550
Modeling Sites with Disaster Recovery in Mind	550
Avoiding Disasters	554
Uninterruptible Power Source	554
RAID	555
Clustering	556
File Replication Service	557
Distributed File Service	558
The Active Directory Database File Structure	558
Backup	560
Creating an Emergency Repair Disk	562
Recovering a Failed Domain Controller	562

Non-Authoritative Restore versus Authoritative Restore	563
Authoritative Restore of Deleted Objects	563
Startup Options	564
The Recovery Console	566
Summary	567
Solutions Fast Track	568
Frequently Asked Questions	570


Appendix A Migrating from Novell NetWare **571**

Migrating from Novell Directory Services	572
Other Utilities	574

Appendix B Secrets **575**

Lesser-Known Management Shortcuts	576
Upgrading DNS and Supporting DNS Dynamic Update Protocol	576
Creating a Custom Microsoft Management Console	576
PDC Emulation and Native Mode	577
How Active Directory Prevents Unnecessary Replication	578
Under-Documented Functions and Procedures	579
How an LDAP Query Accesses Active Directory	579
Software Installation	580
How to Create and Configure a Dfs Root	582
Informational Message	583
Renaming	583
Quick Application of an Updated Group Policy	583
DNS Migrations	584
DNS Best Practices	585
For Experienced Users	586
Add a Server to Two Different Sites Simultaneously	586

A simple domain upgrade process is as follows:

- 
1. Clean up the domain accounts and synchronize.
 2. Take a BDC offline for use in case you need to restore the NT domain.
 3. Upgrade the PDC first.
 4. Upgrade BDCs next.
 5. Once the DCs are all upgraded to Windows 2000, you may switch to native mode at any time, and upgrade member servers to Windows 2000 as needed.

Removing Phantom Objects	586
Phantom Domains	587
Transferring FSMO Roles	588
Troubleshooting Tips	592
Avoiding Errors When Migrating a Domain	592
Remote Procedure Call Errors	592
Index	595