

Mastering™

Robert R. King

Active Directory

Second Edition

Learn How Active Directory Changes
the Way You Manage Your Network

Suranaree University of Technology



91851000651766

Active Directory Concepts,
Installation, and Administration

Updated and Expanded Second Edition



Table of Contents

Introduction

xvii

Part I	The Background and History of Network Directories	1
Chapter 1	An Introduction to Directories	3
	Understanding Network Directories	4
	Traditional Networks vs. Network Directories	8
	Traditional Network Solutions for Common Administrative Tasks	8
	Network Directory-Based Solutions	11
	In Short	13
Chapter 2	Anatomy of a Directory	15
	Paper-Based Directories	16
	Computer-Based Directories	17
	Network Directories	19
	Domain Name System (DNS)	19
	Windows Internet Name Service (WINS)	27
	Novell Directory Services (NDS)	32
	In Short	38
Chapter 3	The X.500 Recommendations	39
	What Is X.500?	41
	The X.500 Recommendations	41
	Developing Uses for a Directory	44
	Designing a Directory	44
	The Schema	45
	Creating a Directory	46
	Hierarchical Structures: X.500 and DOS	51
	The X.500 Hierarchical Structure	53
	In Short	56

Chapter 4	Accessing the Directory	59
	Making Information Available	60
	Accessing the Data	61
	DAP and LDAP	62
	Directory Access Protocol (DAP)	62
	Modifying the Directory	64
	Providing Access to the Directory	65
	What's the Cost?	67
	DAP in Short	69
	Lightweight Directory Access Protocol (LDAP)	69
	How LDAP Differs from DAP	70
	LDAP and DAP: The Similarities	73
	In Short	74
 Part II	 Microsoft Active Directory Services	 75
 Chapter 5	 Microsoft NT without ADS	 77
	What Is a Domain?	79
	Authenticating in NT 4 and Earlier	82
	Primary and Backup Domain Controllers	83
	Member Servers	83
	How PDCs and BDCs Work	84
	The Synchronization Process	85
	Trusts between Domains	87
	Partitioning the Database	88
	Establishing Trust	88
	The Four Domain Models	91
	Single Domain Model	91
	Single-Master Domain Model	92
	Multiple-Master Domain Model	95
	Complete Trust Model	97
	Supporting a Single Logon Account	100
	Allowing Users to Access Resources in Different Domains	101
	In Short	102

Chapter 6	Microsoft NT with ADS	105
	How Networks Develop	106
	The General Goals of ADS	108
	Enterprise Management	110
	An Industry Standard	110
	Vendor Acceptance	111
	User Acceptance	113
	Single Namespace	120
	Namespace	122
	Active Directory Names	123
	Active Directory in the Windows 2000 Server Architecture	125
	The Security Subsystem	127
	The Directory Service Module	128
	The Internal Architecture of the Active Directory Module	130
	In Short	131
Chapter 7	Alphabet Soup: ADS, TCP/IP, DNS, WINS	133
	TCP/IP Basics	134
	The History of TCP/IP	134
	Common TCP/IP Protocols and Tools	135
	TCP/IP Addressing	138
	IP Subnetting	139
	Dynamic Host Configuration Protocol (DHCP)	141
	Installing DHCP Service	144
	How Does DHCP Work?	145
	Domain Name Server (DNS)	158
	So What Exactly Is a DNS Domain?	160
	Planning DNS Naming	161
	Integrating DNS with Active Directory	162
	Installing and Configuring DNS on an ADS Domain Controller	164
	In Short	167

Chapter 8	Building the Active Directory Tree	169
	What Is a Domain?	170
	DNS Domains and NT Domains	171
	Partitioning the Database	174
	Trusts between Domains	176
	Administrative Boundaries	179
	Organizational Units	179
	When to Use a New Domain	182
	Designing the OU Model	183
	What Makes a Good OU Model?	184
	Other Aspects of Planning an OU Model	194
	Trees and Forests	196
	Special Types of ADS Servers	197
	Single Master Functions	199
	In Short	202
Chapter 9	Implementing Your Design	203
	Installing ADS	204
	Before You Begin	205
	The ADS Installation Wizard	207
	Creating Organizational Units	212
	Delegating Administration	214
	Creating Users	219
	Creating a New User Account	220
	Creating Groups	231
	Types of Groups	232
	Access Tokens	232
	Scopes of Groups	233
	The Mechanics of Creating Groups	234
	Creating Printers	238
	Printers in Windows 2000 Server	238
	Non-Windows 2000 Printers	241

	Creating Other Objects	241
	Computer Objects	242
	Contact Objects	243
	Share Objects	244
	In Short	246
Chapter 10	Securing the Active Directory Database	247
	Security Basics	249
	System Identifiers (SIDs)	249
	Access Control List (ACL)	251
	Ownership	254
	Delegating Control	255
	Authentication Security	257
	Kerberos Basics	259
	Public-Key Security	261
	Certificates	263
	In Short	264
Chapter 11	Implementing Group Policies	265
	What Are Group Policies?	266
	Microsoft Management Console	268
	Policy Objects in ADS	271
	Computer Configuration	272
	User Configuration	273
	Using Computer and User Configuration	273
	Software Settings Node	275
	Computer Configuration Node	278
	Computer Configuration\Windows Settings	279
	Computer Configuration\Administrative Templates	282
	User Configuration	285
	User Configuration\Windows Settings	285
	User Configuration\Administrative Templates	286

Configuring Group Policy Settings	287
The Three-Way Toggle	287
Setting Amounts	288
Creating Lists	289
Determining Which Policy Will Be Applied	289
The Order in Which Policies Are Applied	290
Creating Policy Objects	292
Linking Policies to Containers	297
Taking Control	298
In Short	305

Chapter 12 Modifying the Active Directory Schema 307

Schema Basics	308
What's in a Schema?	308
The Active Directory Schema	311
Who Can Modify the Schema?	312
What Can Be Modified?	313
What Cannot Be Modified?	316
Modifying the Schema	316
What Happens When the Schema Is Modified?	317
Preparing for Schema Modifications	317
The Five Types of Schema Modifications	326
In Short	333

Chapter 13 Understanding and Controlling ADS Sites and Replication 335

Understanding Active Directory Sites	337
Determining Site Boundaries	338
Domain Controller Placement Strategies	341
The Default Placement	344
Implementing Active Directory Sites	345
Creating Sites	346
Creating Subnets	348
Creating Site Links	349

	Site Link Bridges	354
	Connection Objects	355
	Understanding Replication	356
	Replication vs. Synchronization	357
	Types of Replication	358
	Behind the Scenes of Replication	360
	Update Sequence Numbers	360
	Propagation Dampening	364
	In Short	365
Part III	The Future of Active Directory Services	367
Chapter 14	ADS and BackOffice	369
	How Might ADS Affect Microsoft BackOffice?	371
	Exchange Server	372
	Proxy Server	375
	Site Server	376
	Systems Management Server (SMS)	378
	SQL Server	381
	Office 2000	381
	In Short	382
Chapter 15	ADS and Third-Party Products	383
	Software	384
	The Application as an Object	385
	Location of Program Files	386
	Licensing	388
	Authentication	389
	Upgrades	389
	Installation	390
	External Access through LDAP	390
	Reporting Features	391
	Software in Short	392

Hardware	392
Hardware as Objects	393
Computer Objects	394
Network Components	396
Printers	397
Fax Services	399
PBX Services	399
Inventory Control	400
Facilities Management	401
In Short	401
Chapter 16	Directory-Enabled Networks (DENs)
	403
Challenges in Today's Networking Environments	405
What Is DEN?	408
Increasing Efficiency and Consistency	408
The DEN Information Model	410
What's in the DEN Information Model?	410
Interoperability	411
DEN Operational Models	411
Defining Objects	414
X.500	415
Common Information Model (CIM)	416
DEN Object Classes	418
NetworkService	418
NetworkProtocol	420
NetworkElement	420
Policy	421
Profile	423
NetworkMedia	424
In Short	425
Appendices	427
Appendix A	429
<i>Index</i>	491