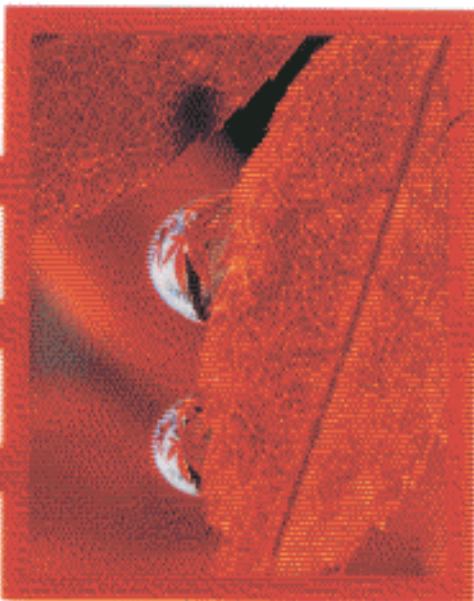


MASTERING™ ACTIVE DIRECTORY

ROBERT R. KING



GET A PREVIEW OF ACTIVE DIRECTORY SERVICES, WINDOWS 2000'S KEY NEW TECHNOLOGY

LEARN HOW ACTIVE DIRECTORY SERVICES WILL CHANGE THE WAY YOU MANAGE YOUR NETWORK

UNDERSTAND ACTIVE DIRECTORY CONCEPTS, IMPLEMENTATION, AND ADMINISTRATION

BASED ON A PRELIMINARY RELEASE OF WINDOWS 2000

Suranaree University of Technology



31051000640012

Table of Contents

Introduction

xix

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	41
	What Is X.500?	43
	The X.500 Recommendations	43
	Developing Uses for a Directory	46
	Designing a Directory	46
	The Schema	47
	Creating a Directory	48
	Hierarchical Structures: X.500 and DOS	53
	The X.500 Hierarchical Structure	55
	In Short	58

Chapter 4	Accessing the Directory	61
	Making Information Available	62
	Accessing the Data	63
	DAP and LDAP	64
	Directory Access Protocol	64
	Modifying the Directory	66
	Providing Access to the Directory	67
	What's the Cost?	69
	DAP in Short	71
	Lightweight Directory Access Protocol (LDAP)	71
	How LDAP Differs from DAP	72
	LDAP and DAP: The Similarities	75
	In Short	76
Part II	Microsoft Active Directory Services	77
Chapter 5	Microsoft NT without ADS	79
	What Is a Domain?	81
	Authenticating in NT 4 and Earlier	84
	Primary and Backup Domain Controllers	85
	Member Servers	85
	How PDCs and BDCs Work	86
	The Synchronization Process	87
	Trusts between Domains	89
	Partitioning the Database	90
	Establishing Trust	90
	The Four Domain Models	93
	Single Domain Model	93
	Single-Master Domain Model	94
	Multiple-Master Domain Model	97
	Complete Trust Model	99
	Supporting a Single Logon Account	102
	Allowing Users to Access Resources in Different Domains	103
	In Short	104

Chapter 6	Microsoft NT with ADS	107
	How Networks Develop	108
	The General Goals of ADS	111
	Enterprise Management	112
	An Industry Standard	112
	<i>Vendor Acceptance</i>	113
	User Acceptance	115
	Single Namespace	118
	Namespace	120
	Active Directory Names	121
	Active Directory in the Windows 2000 Server Architecture	123
	The Security Subsystem	124
	The Directory Service Module	126
	The Internal Architecture of the Active Directory Module	128
	In Short	129
Chapter 7	Alphabet Soup: ADS, TCP/IP, DNS, WINS	131
	TCP/IP Basics	132
	<i>The History of TCP/IP</i>	132
	Common TCP/IP Protocols and Tools	133
	TCP/IP Addressing	135
	IP Subnetting	136
	Dynamic Host Configuration Protocol (DHCP)	139
	Installing DHCP	142
	How Does DHCP Work?	143
	Problems with DHCP	148
	Domain Name Server (DNS)	149
	So What Exactly Is a DNS Domain?	150
	Planning DNS Naming	151
	Integrating DNS with Active Directory	153
	Installing and Configuring DNS on an ADS Domain Controller	154
	In Short	156

Chapter 8	Building the Active Directory Tree	157
	What Is a Domain?	158
	DNS Domains and NT Domains	160
	Partitioning the Database	161
	Trusts between Domains	164
	Administrative Boundaries	166
	Organizational Units	167
	When to Use a New Domain	170
	Designing the OU Model	171
	What Makes a Good OU Model?	172
	Other Aspects of Planning an OU Model	182
	In Short	183
Chapter 9	Implementing Your Design	185
	Installing ADS	186
	Before You Begin	187
	The ADS Installation Wizard	188
	Creating Organizational Units	195
	Delegating Administration	197
	Creating Users	201
	Creating a New User Account	202
	Creating Groups	210
	Types of Groups	210
	Access Tokens	211
	Scopes of Groups	211
	The Mechanics of Creating Groups	212
	Creating Printers	216
	Printers in Windows 2000 Server	217
	Non-Windows 2000 Printers	219
	Creating Other Objects	220
	Computer Objects	221

	Contact Objects	222
	Share Objects	223
	In Short	225
Chapter 10	Securing the Active Directory Database	227
	Security Basics	229
	System Identification Numbers (SIDs)	229
	Access Control List (ACL)	231
	Ownership	234
	Delegating Control	235
	Authentication Security	237
	Kerberos Basics	239
	Public-Key Security	240
	Certificates	243
	In Short	244
Chapter 11	Implementing Group Policies	245
	What Are Group Policies?	246
	Policy Objects in ADS	248
	Software Policies	250
	Software Management	262
	User Documents and Settings	263
	Security Settings	265
	Configuring Group Policies	267
	Editing Group Policies	268
	In Short	268
Chapter 12	Modifying the Active Directory Schema	269
	Schema Basics	270
	What's in a Schema?	270

The Active Directory Schema	273
Who Can Modify the Schema?	275
What Can Be Modified?	275
What Cannot Be Modified?	278
Modifying the Schema	278
What Happens When the Schema Is Modified?	279
Preparing for Schema Modifications	280
The Five Types of Schema Modifications	288
In Short	294

Chapter 13	Understanding and Controlling ADS Sites and Replication	297
	Understanding Active Directory Sites	299
	Determining Site Boundaries	300
	Domain Controller Placement Strategies	303
	The Default Placement	306
	Implementing Active Directory Sites	307
	Creating Sites	308
	Creating Subnets	308
	Creating Site Links	311
	Site Link Bridges	315
	Connection Objects	317
	Understanding Replication	318
	Replication vs. Synchronization	319
	Types of Replication	320
	Behind the Scenes of Replication	322
	Update Sequence Numbers	322
	Propagation Dampening	325
	In Short	327

Part III	The Future of Active Directory Services	329
Chapter 14	ADS and BackOffice	331
	How Might ADS Affect Microsoft BackOffice?	333
	Exchange Server	334
	Proxy Server	336
	Site Server	338
	Systems Management Server (SMS)	339
	SNA Server	342
	SQL Server	342
	Office 2000	343
	In Short	344
Chapter 15	ADS and Third-Party Products	345
	Software	346
	The Application as an Object	347
	Location of Program Files	348
	Licensing	350
	Authentication	351
	Upgrades	351
	Installation	351
	External Access through LDAP	352
	Reporting Features	353
	Software in Short	354
	Hardware	354
	Hardware as Objects	355
	Computer Objects	356
	Network Components	358
	Printers	358
	Fax Services	360
	PBX Services	361
	Inventory Control	362

	Facilities Management	362
	In Short	363
Chapter 16	Directory-Enabled Networks (DEN)	365
	Challenges in Today's Networking Environments	367
	What Is DEN?	370
	Increasing Efficiency and Consistency	370
	The DEN Information Model	371
	What's in the DEN Information Model?	372
	Interoperability	373
	DEN Operational Models	373
	Defining Objects	375
	X.500	376
	Common Information Model (CIM)	377
	DEN Object Classes	379
	NetworkService	380
	NetworkProtocol	381
	NetworkElement	382
	Policy	383
	Profile	385
	NetworkMedia	386
	In Short	386
Appendix A	The Active Directory Schema	389
	Available Attributes	391
	Object Classes	415
	The aCSPolicy Class	415
	The aCSSubnet Class	419
	The addin Class	421
	The addressBookContainer Class	423
	The addressTemplate Class	425
	The addrType Class	427

The adminExtension Class	429
The applicationProcess Class	431
The applicationSettings Class	433
The attributeSchema Class	435
The builtinDomain Class	437
The categoryRegistration Class	440
The certificationAuthority Class	442
The classRegistration Class	444
The classSchema Class	446
The classStore Class	449
The computer Class	451
The configuration Class	457
The connectionPoint Class	459
The container Class	461
<i>Index</i>	464