

# Active Directory™ Programming

THE AUTHORITATIVE SOLUTION

## MASTER THE CONCEPTS

- Understand Active Directory's structure, components, and schema
- Learn to create Active Directory-aware applications
- Understand the use of ADSI and LDAP in Active Directory programming

## BUILD THE APPLICATIONS

- Create robust, full-featured applications with Active Directory integration
- Build applications to access users, groups, and organizations with ADSI
- Enable your applications to search Active Directory using ADSI
- Use LDAP to add, delete, and compare Active Directory objects
- Enable your applications to modify Active Directory using LDAP

## FOREWORD BY

Peter Houston  
Lead Product Manager for Active Directory  
Microsoft Corporation

Suranaree University of Technology



31051000650909

**SAMS**

# Contents

## INTRODUCTION 1

## PART I ACTIVE DIRECTORY FUNDAMENTALS 3

### 1 AN INTRODUCTION TO NETWORK DIRECTORIES 5

|                                                   |    |
|---------------------------------------------------|----|
| What's a Directory? .....                         | 5  |
| Simple Directories .....                          | 5  |
| Application Directories .....                     | 6  |
| Standalone Network Directories .....              | 6  |
| NOS-Integrated Directories .....                  | 6  |
| Global Directories .....                          | 6  |
| 1999—The Year of the Directory? .....             | 7  |
| Why Directories? .....                            | 8  |
| Single Sign-on .....                              | 8  |
| Security .....                                    | 8  |
| Device Identification and Location .....          | 9  |
| Location Independence .....                       | 9  |
| Global Address Book .....                         | 10 |
| Simplified Administration .....                   | 10 |
| Reliability .....                                 | 10 |
| Quality of Service and the DEN Initiative .....   | 10 |
| Directories—The Technical Challenge .....         | 11 |
| The Requirements for a Successful Directory ..... | 11 |
| The Solutions .....                               | 12 |

### 2 AN INTRODUCTION TO ACTIVE DIRECTORY 15

|                                                         |    |
|---------------------------------------------------------|----|
| Active Directory: The Directory for Windows 2000 .....  | 15 |
| Standards-Based .....                                   | 16 |
| Scalable .....                                          | 17 |
| Secure .....                                            | 17 |
| <i>Integrated and Integratable</i> .....                | 17 |
| Extensible Schema .....                                 | 18 |
| Backward-Compatible .....                               | 18 |
| Integration with Windows 2000 .....                     | 19 |
| Integration with Other Microsoft Products .....         | 19 |
| Microsoft Exchange .....                                | 19 |
| Zero Administration Windows and Active Directory .....  | 19 |
| Integration with Other Directory Services .....         | 20 |
| Active Directory Versus Windows NT 4 Domains .....      | 21 |
| Active Directory Versus Novell Directory Services ..... | 23 |

### 3 THE COMPONENTS OF ACTIVE DIRECTORY 25

|                                                   |    |
|---------------------------------------------------|----|
| The Logical Structure of Active Directory .....   | 25 |
| Active Directory Is a Collection of Objects ..... | 25 |
| Classes of Objects .....                          | 26 |

|                                                                  |    |
|------------------------------------------------------------------|----|
| Attributes and Values .....                                      | 26 |
| The Active Directory Schema .....                                | 28 |
| The Directory Information Tree .....                             | 29 |
| Identifying Directory Objects .....                              | 30 |
| Organizing the Directory Tree .....                              | 32 |
| The Root Domain, Domain Trees, and Forests .....                 | 34 |
| The Domain Naming System and Active Directory Domains .....      | 35 |
| The Physical Structure of Active Directory .....                 | 37 |
| Domain Controllers .....                                         | 37 |
| Partitions and Replicas .....                                    | 37 |
| Global Catalogs .....                                            | 37 |
| Active Directory Replication .....                               | 38 |
| Active Directory Sites .....                                     | 38 |
| <b>4 ACTIVE DIRECTORY SECURITY 41</b>                            |    |
| Overview of Windows 2000 Security .....                          | 41 |
| The Features of Windows 2000 Security .....                      | 41 |
| The Components of Windows 2000 Security .....                    | 42 |
| Default Access Rights .....                                      | 66 |
| Evaluating Access Rights .....                                   | 67 |
| Windows 2000 Security and Active Directory .....                 | 68 |
| Domain Controllers and the Local Security Authority .....        | 68 |
| Active Directory Domains .....                                   | 69 |
| Domain Trusts .....                                              | 69 |
| Access Rights Inheritance .....                                  | 70 |
| Default Access Rights .....                                      | 71 |
| Default Owner .....                                              | 72 |
| Property and Property Group Access Rights .....                  | 73 |
| Extending Windows 2000 Security with Private Object Security.... | 73 |
| Security Descriptors as Strings .....                            | 76 |
| Programming Active Directory Security .....                      | 80 |
| Active Directory Security Attributes .....                       | 80 |
| Active Directory Security and LDAP .....                         | 81 |
| Active Directory Security and ADSI .....                         | 81 |
| <b>5 ACTIVE DIRECTORY AND DNS 83</b>                             |    |
| The Origins of DNS and DNS Basics .....                          | 83 |
| DNS Domains .....                                                | 84 |
| DNS Zones .....                                                  | 85 |
| Host Names .....                                                 | 86 |
| Name Servers .....                                               | 86 |
| Primary and Secondary DNS Servers .....                          | 86 |
| DNS Records .....                                                | 87 |
| Name Resolution .....                                            | 87 |
| Updating DNS .....                                               | 87 |
| Why DNS? .....                                                   | 88 |
| Active Directory and DNS .....                                   | 88 |
| How DNS Defines the Active Directory Domain Structure .....      | 88 |
| Locating Domain Controllers with DNS .....                       | 89 |

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Active Directory: Integrated DNS Servers .....                                   | 93 |
| Finding DNS Zone Information in Active Directory<br>and Where It Is Stored ..... | 94 |

## PART II THE CONTENTS OF ACTIVE DIRECTORY 97

### 6 ACTIVE DIRECTORY OPERATIONAL ATTRIBUTES 99

|                                                          |     |
|----------------------------------------------------------|-----|
| RootDSE .....                                            | 99  |
| configurationNamingContext .....                         | 100 |
| currentTime .....                                        | 101 |
| defaultNamingContext .....                               | 101 |
| dnsHostName .....                                        | 101 |
| dsServiceName .....                                      | 101 |
| highestCommittedUSN .....                                | 102 |
| ldapServiceName .....                                    | 102 |
| namingContexts .....                                     | 102 |
| rootDomainNamingContext .....                            | 102 |
| schemaNamingContext .....                                | 103 |
| serverName .....                                         | 103 |
| subschemaSubentry .....                                  | 103 |
| supportedControl .....                                   | 103 |
| supportedLDAPPolicies .....                              | 104 |
| supportedLDAPVersion .....                               | 104 |
| supportedSASLMechanisms .....                            | 105 |
| Operational Attributes on Active Directory Objects ..... | 105 |
| allowedAttributes .....                                  | 105 |
| allowedAttributesEffective .....                         | 105 |
| allowedChildClasses .....                                | 106 |
| allowedChildClassesEffective .....                       | 106 |
| canonicalName .....                                      | 106 |
| createTimeStamp .....                                    | 106 |
| dITContentRules .....                                    | 107 |
| extendedAttributeInfo .....                              | 107 |
| extendedClassInfo .....                                  | 107 |
| modifyTimeStamp .....                                    | 107 |
| objectClasses .....                                      | 107 |
| sDRightsEffective .....                                  | 107 |

### 7 THE ACTIVE DIRECTORY DOMAIN STRUCTURE 109

|                                 |     |
|---------------------------------|-----|
| LDAP Directory Hierarchy .....  | 109 |
| Container Objects .....         | 110 |
| Leaf Objects .....              | 110 |
| Hierarchical Object Names ..... | 110 |
| Naming Contexts .....           | 111 |
| Partitions and Replicas .....   | 112 |
| Windows NT Domains .....        | 112 |
| Active Directory Domains .....  | 112 |
| Domain Trusts .....             | 113 |

|                                                        |     |
|--------------------------------------------------------|-----|
| DNS Domain.....                                        | 113 |
| Active Directory Trees and Forests .....               | 114 |
| The Root Domain .....                                  | 114 |
| Domain Controllers and Replicas .....                  | 115 |
| Sites .....                                            | 115 |
| <b>8 THE CONFIGURATION NAMING CONTEXT 117</b>          |     |
| A Quick Tour of the Configuration Naming Context ..... | 118 |
| The Configuration Container Object .....               | 118 |
| DisplaySpecifiers .....                                | 120 |
| ExtendedRights .....                                   | 123 |
| LostAndFoundConfig .....                               | 124 |
| Partitions .....                                       | 124 |
| Schema .....                                           | 125 |
| Services .....                                         | 125 |
| Sites .....                                            | 128 |
| WellKnownSecurityPrincipals .....                      | 130 |
| <b>9 THE ACTIVE DIRECTORY SCHEMA 131</b>               |     |
| Introduction to the Active Directory Schema .....      | 131 |
| Class Definitions .....                                | 132 |
| Three Kinds of Class Definitions .....                 | 133 |
| Identifying the Class .....                            | 134 |
| Defining the Attributes of a Class .....               | 135 |
| Defining Containment Relationships .....               | 135 |
| Inheritance in the Active Directory Schema .....       | 136 |
| Defining Class Security .....                          | 137 |
| The classSchema Attributes .....                       | 137 |
| Attribute Definitions .....                            | 140 |
| Identifying the Attribute .....                        | 141 |
| Defining the Attribute's Type .....                    | 142 |
| Indexing and the Global Catalog .....                  | 142 |
| Linked Attributes .....                                | 144 |
| Other Administrative Attributes .....                  | 144 |
| Attribute Syntax .....                                 | 147 |
| The Undefined Syntax .....                             | 148 |
| The DN Syntax .....                                    | 148 |
| The OID Syntax .....                                   | 148 |
| The caseExactString Syntax .....                       | 148 |
| The caseIgnoreString Syntax .....                      | 148 |
| The IA5String Syntax .....                             | 149 |
| The NumericString Syntax .....                         | 149 |
| The ORName Syntax .....                                | 149 |
| The Boolean Syntax .....                               | 149 |
| The Integer Syntax .....                               | 150 |
| The OctetString Syntax .....                           | 150 |
| The GeneralizedTime Syntax .....                       | 150 |
| The DirectoryString Syntax .....                       | 151 |
| The PresentationAddress Syntax .....                   | 151 |

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| The DNWithString Syntax .....                                         | 151 |
| The NTSecurityDescriptor Syntax .....                                 | 151 |
| The INTEGERB Syntax .....                                             | 151 |
| The DNWithBinary Syntax .....                                         | 151 |
| The Sid Syntax .....                                                  | 152 |
| The Aggregate Object .....                                            | 154 |
| attributeTypes .....                                                  | 154 |
| objectClasses .....                                                   | 155 |
| dITContentRules .....                                                 | 156 |
| extendedAttributeInfo .....                                           | 156 |
| extendedClassInfo .....                                               | 157 |
| Investigating the Schema .....                                        | 158 |
| Using LDAP to Search the Schema .....                                 | 158 |
| Using ADSI to Search the Schema .....                                 | 159 |
| Manipulating the Schema .....                                         | 159 |
| Finding the Schema FSMO Master .....                                  | 159 |
| Making Sure the Schema Can Be Changed .....                           | 164 |
| Obtaining OIDs for Schema Extensions .....                            | 164 |
| Why Your Schema Changes Don't Show Up .....                           | 165 |
| Sample Schema Manipulation Programs .....                             | 166 |
| Obtaining the Schema FSMO .....                                       | 166 |
| Adding a New Class to the Schema .....                                | 168 |
| Adding a New Attribute to the Schema .....                            | 168 |
| Disabling a Class in the Schema .....                                 | 174 |
| Disabling an Attribute in the Schema .....                            | 176 |
| <b>10 THE ACTIVE DIRECTORY DOMAIN NAMING CONTEXT 177</b>              |     |
| Active Directory Domains .....                                        | 177 |
| The Builtins Container .....                                          | 178 |
| Local Groups .....                                                    | 178 |
| Global Groups .....                                                   | 178 |
| Universal Groups .....                                                | 178 |
| Attributes of Group Objects .....                                     | 179 |
| The Computers Container .....                                         | 180 |
| Computer Attributes Inherited from the User Class .....               | 180 |
| Other Attributes of the Computer Object .....                         | 182 |
| The ForeignSecurityPrincipals Container .....                         | 183 |
| The foreignSecurityPrincipal Object .....                             | 183 |
| The Infrastructure Object .....                                       | 184 |
| The LostAndFound Container .....                                      | 184 |
| The System Container .....                                            | 185 |
| trustedDomain Objects .....                                           | 185 |
| The RIDManager\$ Object .....                                         | 187 |
| The CN=System,CN=Policies Container<br>and Group Policy Objects ..... | 188 |
| The Users Container .....                                             | 189 |
| User Identification Attributes .....                                  | 191 |
| Security Attributes .....                                             | 193 |
| Login Attributes .....                                                | 194 |
| System Service Attributes .....                                       | 199 |

|                                        |     |
|----------------------------------------|-----|
| The Domain Controllers Container ..... | 199 |
| dNSHostName .....                      | 200 |
| operatingSystem .....                  | 200 |
| operatingSystemHotfix .....            | 200 |
| operatingSystemServicePack .....       | 200 |
| operatingSystemVersion .....           | 200 |
| rIDSetReferences .....                 | 200 |
| serverReferenceBL .....                | 201 |
| servicePrincipalName .....             | 201 |

## PART III ACTIVE DIRECTORY SERVICES INTERFACE 203

### 11 ADSI FUNDAMENTALS 205

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| Introduction to Active Directory Services Interface .....                        | 205 |
| Multiple Client Platforms .....                                                  | 206 |
| Multiple Directory Providers .....                                               | 206 |
| ADSI or LDAP? .....                                                              | 207 |
| Platform .....                                                                   | 207 |
| Language .....                                                                   | 208 |
| Portability Between Directories .....                                            | 209 |
| Other Considerations .....                                                       | 210 |
| Component Object Model (COM) Basics .....                                        | 211 |
| I Know Don Box, and I'm No Don Box .....                                         | 211 |
| What Is COM? .....                                                               | 211 |
| Why COM? .....                                                                   | 212 |
| What's the Big Idea? .....                                                       | 212 |
| The Components of COM .....                                                      | 212 |
| Getting Started with ADSI .....                                                  | 220 |
| Setting Up Your Machine .....                                                    | 220 |
| The "Hello, World" ADSI Program .....                                            | 222 |
| Special COM Data Classes.....                                                    | 226 |
| A Note on Exceptions with <code>_bstr_t</code> and <code>_variant_t</code> ..... | 227 |
| The <code>_bstr_t</code> Class .....                                             | 228 |
| The <code>_variant_t</code> Class .....                                          | 228 |
| The <code>_com_error</code> Class .....                                          | 228 |
| Binding to Active Directory Objects .....                                        | 228 |
| ADsPaths .....                                                                   | 228 |
| Serverless Binding with ADSI .....                                               | 230 |
| Binding to a Directory Object by GUID .....                                      | 231 |
| What Happens When You Bind to a Directory Object? .....                          | 231 |
| Fast Binding with ADSI .....                                                     | 232 |
| Binding with the Helper Functions <code>AdsGetObject()</code> .....              | 232 |
| Binding with the Helper Functions <code>AdsOpenObject()</code> .....             | 237 |
| Binding with the <code>IADsOpenDSObject::OpenDSObject()</code><br>Function ..... | 241 |

### 12 BASIC ACTIVE DIRECTORY ADSI INTERFACES 245

|                                            |     |
|--------------------------------------------|-----|
| The ADSI Directory Object Interfaces ..... | 246 |
| The IADs Interface .....                   | 246 |
| The IADsPropertyList Interface .....       | 271 |

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| The IADsPropertyEntry Interface .....                                                                | 276 |
| The IADsPropertyValue Interface .....                                                                | 277 |
| The IADsPropertyValue2 Interface .....                                                               | 279 |
| The IDirectoryObject Interface .....                                                                 | 279 |
| The IADsContainer Interface .....                                                                    | 287 |
| The IADsDeleteOps Interface .....                                                                    | 303 |
| <b>13 SEARCHING ACTIVE DIRECTORY WITH ADSI 307</b>                                                   |     |
| Introduction to Searching with ADSI .....                                                            | 307 |
| Specifying a Search Base .....                                                                       | 308 |
| Search Filter .....                                                                                  | 308 |
| Specifying Attributes to Return .....                                                                | 309 |
| Objects as Rows .....                                                                                | 309 |
| Attributes as Columns .....                                                                          | 309 |
| The IDirectorySearch Interface .....                                                                 | 309 |
| Starting and Ending a Search with IDirectorySearch .....                                             | 310 |
| Terminating a Search with<br>IDirectorySearch::CloseSearchHandle() .....                             | 313 |
| Retrieving Objects with<br>IDirectorySearch::GetNextRow() .....                                      | 314 |
| Retrieving Attributes with IDirectorySearch::GetNextCol()<br>and IDirectorySearch::GetColumn() ..... | 316 |
| A Simple Search Using IDirectorySearch .....                                                         | 319 |
| Extended Searches Using Search Preferences .....                                                     | 322 |
| Synchronous and Asynchronous Searching with<br>IDirectorySearch .....                                | 327 |
| Paged Searches Using IDirectorySearch .....                                                          | 329 |
| Sorting Search Results with IDirectorySearch .....                                                   | 330 |
| Enabling and Disabling the Results Cache with<br>IDirectorySearch .....                              | 333 |
| Setting Limits on Searches with IDirectorySearch .....                                               | 334 |
| <b>14 ACCESSING USERS, GROUPS, AND ORGANIZATIONS WITH ADSI 341</b>                                   |     |
| Accessing User Objects with ADSI .....                                                               | 342 |
| The IADsUser Interface .....                                                                         | 342 |
| Getting a User's Name with IADsUser .....                                                            | 347 |
| Locking a User Account with IADsUser .....                                                           | 350 |
| Setting a User Password with IADsUser .....                                                          | 352 |
| Accessing Groups with ADSI .....                                                                     | 353 |
| The IADsGroup Interface .....                                                                        | 354 |
| The IADsMembers Interface .....                                                                      | 359 |
| Accessing Organizations, Localities, and Organizational<br>Units with ADSI .....                     | 367 |
| The IADsO, IADsOU, and IADsLocality Interfaces .....                                                 | 367 |
| Getting the Description of an Organization .....                                                     | 369 |
| Enumerating the Contents of an O or OU .....                                                         | 371 |



|           |                                                                  |            |
|-----------|------------------------------------------------------------------|------------|
| <b>15</b> | <b>ACCESSING THE ACTIVE DIRECTORY SCHEMA WITH ADSI</b>           | <b>373</b> |
|           | A Tale of Two Schemas .....                                      | 373        |
|           | Which Version of the Schema Should You Use? .....                | 374        |
|           | Using the Generic Object Interfaces to Access the Schema .....   | 374        |
|           | Enumerating Classes in the Schema Using the Generic              |            |
|           | Object Interfaces .....                                          | 375        |
|           | Binding to the Schema Master .....                               | 378        |
|           | Adding a New Attribute Using the Generic Object Interfaces ..... | 381        |
|           | Adding a New Class Using the Generic Object Interfaces .....     | 384        |
|           | Using the Abstract Schema Interface to Access the Schema .....   | 387        |
|           | Binding to the Abstract Schema .....                             | 388        |
|           | Using the Abstract Schema Container Interface .....              | 389        |
|           | Accessing a Schema Class Object with IADsClass .....             | 391        |
|           | Accessing a Schema Property Object with IADsProperty .....       | 396        |
|           | Accessing a Schema Syntax Object with IADsSchema .....           | 398        |
| <b>16</b> | <b>OTHER ACTIVE DIRECTORY API FUNCTIONS</b>                      | <b>403</b> |
|           | Connecting to an Active Directory Service .....                  | 404        |
|           | Translating Directory Service Names .....                        | 406        |
|           | Discovering Sites, Servers, and Domains .....                    | 411        |
|           | Finding a Domain Controller .....                                | 411        |
|           | Listing the Sites in Active Directory .....                      | 417        |
|           | Listing the Servers in a Site .....                              | 419        |

## **PART IV: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL 423**

|           |                                                             |            |
|-----------|-------------------------------------------------------------|------------|
| <b>17</b> | <b>LDAP FUNDAMENTALS</b>                                    | <b>425</b> |
|           | LDAP History .....                                          | 426        |
|           | LDAP Version 1 .....                                        | 426        |
|           | LDAP Version 2 .....                                        | 427        |
|           | LDAP Version 3 .....                                        | 427        |
|           | Installing the LDAP Components .....                        | 427        |
|           | LDAP Programming Components .....                           | 429        |
|           | WINLDAP.H .....                                             | 429        |
|           | WLDAP32.LIB .....                                           | 429        |
|           | WLDAP32.DLL .....                                           | 429        |
|           | Setting Up Visual Studio for LDAP Programming .....         | 429        |
|           | Method One: Modify the Project Settings .....               | 429        |
|           | Method Two: Modify the Visual C++ Directories Options ..... | 431        |
|           | Method Three: Modify the System Environment Variables ..... | 432        |
|           | LDAP Programming Model .....                                | 433        |
|           | Initializing the Client Library .....                       | 434        |
|           | Connecting to an Active Directory Server .....              | 434        |
|           | Issuing LDAP Requests .....                                 | 434        |
|           | Processing LDAP Results .....                               | 435        |
|           | Closing the Connection .....                                | 435        |
|           | Some General Notes About LDAP Programming for               |            |
|           | Active Directory .....                                      | 435        |
|           | Creating an LDAP Connection .....                           | 435        |
|           | Error Handling .....                                        | 436        |

|                                                                              |     |
|------------------------------------------------------------------------------|-----|
| ANSI and Unicode Character Sets .....                                        | 436 |
| Object Identifiers (OIDs) .....                                              | 437 |
| Synchronous and Asynchronous (Multithreaded) Functions .....                 | 438 |
| A Simple LDAP Program .....                                                  | 439 |
| <b>18 CONNECTING TO ACTIVE DIRECTORY WITH LDAP 443</b>                       |     |
| A Note About Using the LDAP Client Library .....                             | 444 |
| Locating a Domain Controller .....                                           | 446 |
| Initializing the LDAP Client Library .....                                   | 451 |
| The <code>ldap_init()</code> Function .....                                  | 452 |
| A Note on Port Numbers .....                                                 | 454 |
| The <code>ldap_sslinit()</code> Function .....                               | 454 |
| Connecting to the Domain Controller .....                                    | 456 |
| The <code>ldap_connect()</code> Function .....                               | 456 |
| The <code>ldap_open()</code> Function .....                                  | 458 |
| Connecting with UDP Using the <code>cldap_open()</code> Function .....       | 459 |
| Disconnecting from an Active Directory Domain Controller .....               | 462 |
| <b>19 AUTHENTICATING WITH ACTIVE DIRECTORY 465</b>                           |     |
| Authentication Credentials .....                                             | 465 |
| Multiple Binds .....                                                         | 466 |
| Anonymous Connections .....                                                  | 466 |
| LDAP Binding Functions .....                                                 | 466 |
| Simple LDAP Binding with <code>ldap_simple_bind_s()</code> .....             | 467 |
| Using SASL to Authenticate with Active Directory .....                       | 470 |
| Using <code>ldap_bind_s()</code> to Authenticate with Active Directory ..... | 472 |
| <b>20 SEARCHING ACTIVE DIRECTORY WITH LDAP 477</b>                           |     |
| Specifying an LDAP Search .....                                              | 478 |
| The Starting Point of the Search .....                                       | 478 |
| Search Depth .....                                                           | 478 |
| Search Criteria .....                                                        | 479 |
| Requesting Attributes .....                                                  | 479 |
| A Simple Search Using <code>ldap_search_s()</code> .....                     | 480 |
| Processing the Search Results .....                                          | 481 |
| Iterating the Returned Entries .....                                         | 482 |
| Getting the Distinguished Name of a Returned Entry .....                     | 483 |
| Retrieving the Returned Attributes .....                                     | 484 |
| Processing the Attribute Values .....                                        | 486 |
| Processing Binary Attribute Values .....                                     | 490 |
| Searching with a Timeout Value .....                                         | 494 |
| <b>21 ADVANCED SEARCHING WITH LDAP 499</b>                                   |     |
| Complex Search Criteria .....                                                | 499 |
| How LDAP Processes Search Filters .....                                      | 500 |
| The Full LDAP Search Filter Syntax .....                                     | 500 |
| Searching for Bit-Field Attributes .....                                     | 515 |
| Checking the Validity of an LDAP Search Filter .....                         | 516 |

|                                                             |     |
|-------------------------------------------------------------|-----|
| Asynchronous LDAP Searches .....                            | 517 |
| Starting an Asynchronous Search .....                       | 519 |
| Processing Asynchronous Search Results .....                | 520 |
| Abandoning an Asynchronous Search.....                      | 528 |
| Attribute Requests .....                                    | 532 |
| Requesting All Attributes .....                             | 532 |
| Requesting Specific Attributes .....                        | 532 |
| Requesting Operational Attributes .....                     | 533 |
| Requesting All Attributes and Operational Attributes .....  | 534 |
| Requesting No Attributes .....                              | 535 |
| Time-Limited LDAP Searches .....                            | 535 |
| Setting a Server Time Limit for a Search .....              | 536 |
| Setting a Client Time Limit for a Search .....              | 540 |
| Changing the Server Search Time Limits .....                | 543 |
| Entry-Limited LDAP Searches .....                           | 543 |
| Why Entry Limits Aren't .....                               | 544 |
| Setting Search Entry Limits .....                           | 544 |
| <b>22 EXTENDING LDAP SEARCHES 547</b>                       |     |
| Extending LDAP Searches with LDAP Controls .....            | 547 |
| Client and Server Controls .....                            | 548 |
| The LDAPControl Structure .....                             | 548 |
| The Extended LDAP Functions .....                           | 549 |
| Introduction to Active Directory Search Controls .....      | 549 |
| Getting Notifications of Directory Changes .....            | 550 |
| Searching for Deleted Objects .....                         | 555 |
| Retrieving Security Descriptors for Directory Objects ..... | 558 |
| Retrieving Extended Name Information .....                  | 563 |
| Getting Search Results—A Page at a Time .....               | 566 |
| Two Ways to Perform a Paged Search .....                    | 566 |
| Setting Up the Paged Search .....                           | 567 |
| Retrieving Pages of Entries .....                           | 569 |
| Abandoning a Paged Search .....                             | 573 |
| Getting Search Results in Sorted Order .....                | 574 |
| Sorting Oddities and Limitations .....                      | 574 |
| The Sorted Search Functions .....                           | 576 |
| Using Paged and Sorted Searches Together .....              | 590 |
| <b>23 PROCESSING LDAP REFERRALS 599</b>                     |     |
| Two Kinds of Referrals .....                                | 600 |
| When Are Referrals Generated? .....                         | 601 |
| Two Strategies for Handling Referrals .....                 | 602 |
| Configuring the LDAP Client to Chase Referrals .....        | 602 |
| Chasing Referrals from Search Results .....                 | 604 |
| Caching Connections for Referrals .....                     | 617 |
| <b>24 MODIFYING ACTIVE DIRECTORY OBJECTS WITH LDAP 625</b>  |     |
| Things to Know Before You Go .....                          | 626 |
| Multiple Modification Operations .....                      | 627 |
| Multivalued Attributes .....                                | 627 |

|                                                                            |     |
|----------------------------------------------------------------------------|-----|
| Modification Operations .....                                              | 627 |
| No Empty Attributes .....                                                  | 627 |
| Schema Rules .....                                                         | 627 |
| Access Rights .....                                                        | 629 |
| Data Structures for Modifying Objects with LDAP .....                      | 629 |
| Selecting the Appropriate API Function .....                               | 630 |
| API Data Structures for Modifying Objects with LDAP .....                  | 631 |
| The <code>berval</code> Structure .....                                    | 631 |
| The <code>ldapmod</code> Structure .....                                   | 631 |
| Modifying an Existing Attribute .....                                      | 633 |
| Adding a New Attribute to an Existing Object.....                          | 636 |
| Adding a New Attribute Using the <code>berval</code> Structure .....       | 639 |
| Deleting an Existing Attribute .....                                       | 642 |
| Adding Additional Values to an Existing Attribute .....                    | 645 |
| Deleting a Value from a Multivalued Attribute .....                        | 646 |
| Performing Bulk Directory Updates with the                                 |     |
| Lazy Commit Control .....                                                  | 649 |
| Asynchronous Directory Modifications .....                                 | 654 |
| Retrieving the Results of an Asynchronous Modification .....               | 658 |
| Using Asynchronous Search and Modifications Together .....                 | 661 |
| Moving and Renaming Active Directory Objects .....                         | 666 |
| Renaming an Active Directory Object with LDAP .....                        | 668 |
| Renaming Active Directory Objects Asynchronously .....                     | 670 |
| <b>25 ADDING ACTIVE DIRECTORY OBJECTS WITH LDAP 675</b>                    |     |
| Things to Know Before You Go .....                                         | 676 |
| Adding Objects Is a Lot Like Modifying Them .....                          | 676 |
| Adding Multiple Attributes at Once .....                                   | 677 |
| Multivalued Attributes .....                                               | 677 |
| Existence of the Parent Container .....                                    | 677 |
| Schema Rules .....                                                         | 677 |
| API Data Structures for Adding Objects with LDAP .....                     | 680 |
| The <code>berval</code> Structure .....                                    | 681 |
| The <code>ldapmod</code> Structure .....                                   | 681 |
| Selecting the Appropriate API Function .....                               | 683 |
| Adding Objects Synchronously by Using <code>ldap_add_s()</code> .....      | 683 |
| Adding Objects Asynchronously by Using <code>ldap_add()</code> .....       | 687 |
| Retrieving the Results of an Asynchronous Addition .....                   | 689 |
| Adding Objects in Bulk by Using the Lazy Commit Control .....              | 696 |
| Adding Objects to the Directory with <code>ldap_add_ext_s()</code> .....   | 701 |
| <b>26 DELETING ACTIVE DIRECTORY OBJECTS WITH LDAP 705</b>                  |     |
| Things to Know Before You Go .....                                         | 706 |
| Access Rights .....                                                        | 706 |
| Containers Must Be Empty Before You Can Delete Them .....                  | 706 |
| Selecting the Appropriate API Function .....                               | 706 |
| Deleting Objects Synchronously by Using <code>ldap_delete_s()</code> ..... | 707 |
| Deleting a Container and Its Subordinate Objects                           |     |
| Using <code>ldap_delete_ext_s()</code> .....                               | 709 |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| Deleting Objects Asynchronously Using <code>ldap_delete()</code> .....                           | 712 |
| Retrieving the Results of an Asynchronous Deletion .....                                         | 714 |
| Deleting Objects Asynchronously Using LDAP<br>Controls with <code>ldap_delete_ext()</code> ..... | 720 |
| <b>27 COMPARING ACTIVE DIRECTORY OBJECTS WITH LDAP 725</b>                                       |     |
| Things to Know Before You Go .....                                                               | 726 |
| The Differences Between Compare and Search .....                                                 | 726 |
| Matching Rules .....                                                                             | 727 |
| Access Rights .....                                                                              | 727 |
| Comparing Binary Values .....                                                                    | 727 |
| Testing Multivalued Attributes .....                                                             | 727 |
| Using <code>ldap_compare_s()</code> to Test Attribute Assertions .....                           | 727 |
| Using <code>ldap_compare_ext_s()</code> to Test Attribute Assertions .....                       | 730 |
| Using <code>ldap_compare()</code> to Test Attribute Assertions .....                             | 734 |
| Retrieving the Results of an Asynchronous Comparison .....                                       | 737 |
| Using <code>ldap_compare_ext()</code> to Test Attribute Assertions .....                         | 743 |
| <b>28 EXTENDING LDAP WITH OPTIONS AND CONTROLS 749</b>                                           |     |
| LDAP Options .....                                                                               | 750 |
| Reading the Options .....                                                                        | 750 |
| Setting the Options .....                                                                        | 751 |
| Turning Options On and Off .....                                                                 | 752 |
| "Standard" LDAP Options .....                                                                    | 752 |
| LDAP_OPT_DESC .....                                                                              | 752 |
| LDAP_OPT_DEREF .....                                                                             | 753 |
| LDAP_OPT_SIZELIMIT .....                                                                         | 754 |
| LDAP_OPT_TIMELIMIT .....                                                                         | 754 |
| LDAP_OPT_REFERRALS .....                                                                         | 755 |
| LDAP_OPT_RESTART .....                                                                           | 756 |
| LDAP_OPT_PROTOCOL_VERSION and<br>LDAP_OPT_VERSION .....                                          | 757 |
| LDAP_OPT_HOST_NAME .....                                                                         | 757 |
| LDAP_OPT_ERROR_NUMBER .....                                                                      | 758 |
| LDAP_OPT_ERROR_STRING .....                                                                      | 758 |
| Microsoft-Specific LDAP Options .....                                                            | 759 |
| LDAP_OPT_SSL .....                                                                               | 759 |
| LDAP_OPT_REFERRAL_HOP_LIMIT .....                                                                | 760 |
| LDAP_OPT_PING_KEEP_ALIVE, LDAP_OPT_PING_WAIT_TIME,<br>and LDAP_OPT_PING_LIMIT .....              | 760 |
| LDAP_OPT_DNSDOMAIN_NAME .....                                                                    | 761 |
| LDAP_OPT_GETDSNAME_FLAGS .....                                                                   | 761 |
| LDAP_OPT_PROMPT_CREDENTIALS .....                                                                | 762 |
| LDAP_OPT_AUTO_RECONNECT .....                                                                    | 762 |
| LDAP_OPT_SOCK_FLAGS .....                                                                        | 762 |

|                                                    |     |
|----------------------------------------------------|-----|
| Get Security Descriptor .....                      | 765 |
| Change Notification (Persistent Search) .....      | 765 |
| Show Deleted Objects .....                         | 766 |
| Lazy Commit .....                                  | 766 |
| DirSync Control .....                              | 766 |
| Return Extended DN .....                           | 767 |
| Tree Delete .....                                  | 767 |
| Cross Domain Move .....                            | 767 |
| Verify Server Name .....                           | 768 |
| Search with Local Scope .....                      | 768 |
| Permissive Modify .....                            | 768 |
| <b>29 LDAP ERROR-HANDLING FUNCTIONS 769</b>        |     |
| Handling LDAP Errors .....                         | 769 |
| LDAP Error Codes .....                             | 770 |
| Getting String Descriptions of LDAP Errors .....   | 775 |
| Converting LDAP Errors to Win32 Errors .....       | 775 |
| <b>PART V APPENDICES 777</b>                       |     |
| <b>A ADSI INTERFACES FOR ACTIVE DIRECTORY 779</b>  |     |
| <b>B MICROSOFT WINDOWS 2000 LDAP FUNCTIONS 799</b> |     |
| <b>INDEX 805</b>                                   |     |