

Index

Note: Italicized locators indicate figures/
tables.

A

- abandon operation, 29, 93–94
- Abstract classes, 107, 114
- Abstract Syntax Notation One (ASN.1), 129
 - attribute syntax, 318
 - format, 317
 - matching rules, 324
 - object class syntax, 318
- Access control entries, 183, 221, 264
- Access control factors, 182, 196, 222
- Access control information, 332, 333, 366–368
- Access control instruction, 307
- Access control list, 180, 221, 307, 332
 - Active Directory, 264, 266
- Access control policy, 182, 183
- Access controls, 207
 - and impersonation, 220
 - and naming attributes, 61
 - and roles, 293
- <access> directives, 221, 344–345
- Access rights, 182
- ACEs. *See* Access control entries
- ACI. *See* Access control information; Access control instruction
- aci attribute, 307, 367
- ACI bind rules, 360
- ACI expressions, 223
- ACI headings, 360
- ACI permissions, 360, 361
- ACI targets, 307, 341, 358–360
- ACL. *See* Access control list
- Active Directory, 15, 27, 71, 96, 110, 199, 227–269, 309, 333
 - domain tree, 232
 - evaluation of, 267–269
 - forest namespace, 234
 - forest with two domain trees, 233
 - global catalogs with, 169
 - impact of Exchange 2000 on, 250
 - management of, 255–262
 - namespaces for, 228–245
 - naming contexts for, 238
 - operations and clients for, 245–251
 - permissions available in, 264
 - replication, 257, 259
 - schema for, 251–255

- Active Directory, *continued*
 - security with, 262–267
 - strengths of, 267–269
 - well-known security principals with, 265
- Active Directory Application Mode, 269
- Active Directory controls, 351–355
 - ASQ control, 355
 - Change Notification (Psearch) control, 352
 - Cross Domain Move control, 353
 - Directory Synchronization (Dirsync) control, 352–353
 - Get Security Descriptor control, 351
 - Lazy Commit control, 352
 - Paged Search control, 351
 - Permissive Modify control, 354–355
 - Return Extended DN control, 353
 - Search with Local Scope control, 354
 - Server Search Operations control, 354
 - Show Deleted Objects control, 352
 - Sorted Search Request control, 352
 - Sorted Search Response control, 354
 - Statistics control, 353–354
 - Tree Delete control, 353
 - Verify Server Name control, 354
 - Virtual List View Request control, 355
 - Virtual List View Response control, 355
- Active Directory harvester, 336–338
- Active Directory Services Interface, 100, 246, 248, 249, 268
- Active Directory Users and Computers interface, 247
- AD. *See* Active Directory
- AD/AM. *See* Active Directory Application Mode
- add operation, 87–88, 105, 154
- Address Book application, 246–247
- Administrative Console, with Directory Server, 283
- Administrative controls, 139
- Administrative server parameters, 192–193
- ADO.NET, 249
- ADSI. *See* Active Directory Services Interface
 - ADSI Edit, 255, 261
 - alias class, 253
 - Alias entries, 78, 154, 253
 - Aliases, 67, 139, 153–155, 195
 - referrals *versus*, 153–154
 - OpenLDAP support for, 213
 - allowedChildClasses attribute, 252
 - altSecurityIdentities attribute, 254
 - AND operator (&), 75
 - Anonymous clients, 86, 93
 - Application programming interfaces (APIs), 27, 98–100
 - Approximate string match operator (~=), 80
 - ASCII encoding, 30
 - ASN.1. *See* Abstract Syntax Notation One
 - ASQ control, in Active Directory, 355
 - Asterisk (*)
 - and <what> element, 341
 - and regular expressions, 218
 - as wildcard, 80
 - Asynchronous versions, for API functions, 99
 - AttributeDescription, 121, 122, 124
 - Attribute options, 121–126
 - language support and, 123–126
 - OpenLDAP support for, 213
 - Attributes, 38, 116–129, 138
 - in Active Directory schema, 254–255
 - defining, 116–117
 - for delegating impersonation authorization, 219
 - of entry, 7
 - indexing in Active Directory, 259–260
 - and LDAP schema, 104
 - matching rules, 81
 - naming, 57, 58–60, 119–120
 - name synonyms, 119–120
 - in OpenLDAP schema, 213–214
 - operational, 77, 126–129
 - and phone numbers, 60
 - Attribute sets, 265
 - Attribute subtypes, 120–121
 - conceptual example of, 121
 - OpenLDAP support for, 213

- AttributeType, 7, 105, 117
 - attributeTypes attribute, 128
 - elements of, 118–120
 - Attribute Uniqueness plug-in, 303
 - Attribute values, 8, 117
 - for language options, 125
 - in search filters, 74
 - Authentication, 34–36, 39, 94, 179, 180–182, 196, 284
 - with Active Directory, 229, 262–263
 - Anonymous, 181, 217, 305
 - Cleartext, 35, 36, 180
 - CRAM–MD5, 217
 - DIGEST–MD5, 35, 181, 182, 187, 305, 217
 - with Directory Server, 305–307, 364
 - GSSAPI, 217
 - and index directories, 169
 - Kerberos. *See* Kerberos
 - and OpenLDAP, 208
 - PLAIN, 217
 - and public key encryption, 188
 - SASL. *See* Simple Authentication and Security Layer
 - SCRAM–MD5, 217
 - Authentication identity, authorization
 - identity mapped to, 183
 - Authoritative version, of partition, 141
 - Authority Registry, in Stanford Registry, 331
 - Authorization, 34, 35, 180, 182–185, 284
 - with Active Directory, 262, 264–266
 - with Directory Server, 305, 307–308
 - and impersonation, 219
 - with OpenLDAP, 221–222
 - Authorization identity, 184, 342
 - Auxiliary classes, 107
 - inheritance *versus* , 117
 - using, 114–117
- B**
- Backends
 - with OpenLDAP, 216
 - writing, 206
 - Backslash character ([SLASH]), in naming
 - special characters, 62
 - Backus–Naur Form, 19
 - attribute syntax, 319
 - format, 317
 - notation, 129
 - object class syntax, 318–319
 - schema format, 119, 211
 - Bandwidth
 - and replication, 160
 - and sites, 234
 - Base DN, 23
 - baseObject, 73
 - Base scope, 74
 - BER encoding, 27, 129
 - binary option, 122, 123, 125
 - Bindname extension, 64
 - bind operation, 29, 84, 86, 193
 - Bind rules, 307, 360
 - BNF. *See* Backus–Naur Form
 - Browsers, and LDAP, 28
 - Bulk modifications, 195
- C**
- C, 27, 100
 - functions in API of, for LDAP, 314, 315–316
 - SDKs for LDAP API in, 284
 - CA. *See* Certificate authority
 - canonicalName attribute, 253
 - Certificate authority, 186, 190, 254
 - with certificate, 191
 - management, 193
 - Certificates, 180, 189, 190
 - authentication, with Directory Server, 306
 - revocation lists, 186
 - Chaining, 151, 195, 285, 310, 314
 - benefits with, 282
 - Cascading chaining, 281
 - with Directory Server, 280–282
 - and master directories, 167
 - and roles, 292
 - Chaining Loop Detection control, 287
 - Change logs, with Directory Server, 303
 - Change Notification control, 250, 352
 - Chasing the referral, 144, 147

390 Index

- Checksum, 189
- Child entries, and containers, 10, 49
- children attributes, with OpenLDAP, 214
- Child zones, 45
- Classes
 - in Active Directory schema, 252–254
 - in OpenLDAP schema, 212–213
- Class of Service, 293–295, 310
 - Classic CoS, 297–298
 - cosAttribute, for CoS definition entries, 294–295
 - CoS definition entries, 294
 - CoS Specifier, 295
 - CoS template, 295
 - cosTemplate, 296
 - cosTemplate object class, 295
 - Indirect CoS, 298, 300–301
 - Pointer CoS, 296–297
- classSchema object class, 253
- CLDAP. *See* Connectionless LDAP
- Client LDAP operations, 69–101, 313–316
 - client software, 70–71
 - directory-enabled services and applications, 71
 - draft controls, 313–314
 - and parameters, 77–79
 - web-based client interface, 72–76
- Client libraries, OpenLDAP, 202
- Clients, 27–28, 39, 70–71
 - and abandon operation, 93–94
 - and Active Directory, 246–248
 - and add operation, 87
 - and bind operation, 86
 - and chaining, 151
 - and compare operation, 87
 - and Directory Server, 283
 - and LDAP protocol, 83, 84
 - and modifyRN or rename operation, 89
 - and referrals, 144, 145
 - and unbind operation, 93
- Client-server model, 26–27
- Client session operations, 28, 29
- Client tools, with OpenLDAP, 208–209
- Closed source, open source *versus*, 200
- cn attribute, 8, 58, 120, 126, 253
 - cn=config naming context, with Directory Server, 275, 276, 304
 - cn=plugins, with Directory Server, 276
- Code injection, 63
- ColdFusion, 100
- Collisions, 143
 - and Active Directory replication, 258–259
 - Directory Server and resolution of, 303
- COM. *See* Component Object Model
- Comma-separated values, 256
- Commenting, 62
- compare operation, 29, 86–87
- comparison operator, 74, 79
- Component Object Model, 238, 248
- computer object class, in Active Directory, 254
- Computers container, 241–242
- Configuration partition,
 - Active Directory, 236, 238, 239
 - with Directory Server, 275–276
- Configuration parameters
 - with Active Directory, 260–262
 - with Directory Server, 304–305
 - with OpenLDAP, 215–216
- Connectionless LDAP, 85–86
- Connectivity, and sites, 234
- Connectors, 172–173
- Consumer replica, with Directory Server, 302
- Consumers, of data, 164–165
- Containers, 9, 24, 48
 - common object classes used for, 51
 - LDAP, 49
 - referrals for, 154
- Content rules, in object class definition, 104–105
- Continuation references, 148
- controlAccessRights entries, 239
- <control> element, 346
- Controls. *See* LDAP controls
- CoS. *See* Class of Service
- createTimestamp, 119, 213
- creatorsName, 213
- CRLs, 267

- Cross Domain Move control, in Active Directory, 353
- crossRef entry, 239
- CSV. *See* Comma-separated values
- Cyrus Project (Carnegie Mellon University), 216
- D**
- DACL. *See* Discretionary access control list
- DAP. *See* Directory access protocols
- Data, 40
 - duplication of between servers, 34
 - harvesting, 171–174
 - movement of between directories, 174–179
- Data architecture management, 162–166
 - with Active Directory, 260
 - directory synchronization, 169–170
 - harvesting data, 171–174
 - loose directory interconnection, 170
 - master directories, 167–169
 - metadirectories, 166–167
 - privacy concerns, 165–166
 - sources and owners, 162–163
 - subscribers and consumers, 164–165
- Database functionality
 - with Directory Server, 277–278
 - with OpenLDAP, 206
- Databases, directories *versus* , 11–12
- Data brokering, 171
- Data loss, protection against, 33
- Data manipulation, integration and, 34
- Data values, matching rules for comparing, 130
- dc attribute, 23, 47, 134
- dcObject object class, 134
- Decryption, 187–188
- Default indexes, with Directory Server, 279
- Default referrals, 147, 148, 149, 150, 280
- Default schema, 31
- delete operation, 88, 154
- Denial of service attacks, 193
- derefAliases, 78
- derefAlways, 78
- Dereferencing aliases, 78, 155
- derefFindingBaseObj, 78
- derefInSearching, 78
- DER encoding, 129
- Diagramming directory namespaces, 53
- Digital certificates, 35, 123
- Digital signatures, 189–190
- Directories, xix
 - benefits with, 16–17
 - binding to, 86
 - and businesses, 6–8
 - databases *versus* , 11–12
 - data movement between, 174–179
 - distributed, 33–34
 - introduction to, 3–5
 - namespaces in, 21–26
 - people friendly, 66
 - security for, 179–193
 - structuring, 55–56
 - typical use of, 13–16
- Directory access protocols, 26, 106
- Directory access rights, 183
- Directory administrators, and privacy restrictions, 166
- Directory architecture, and referrals, 145
- Directory-enabled applications, 71
 - with Directory Server, 283–284
 - with OpenLDAP, 209
- Directory-enabled services, 71
 - with Active Directory, 249–251
 - few boundaries with, 72
- Directory entries, SASL authentication identities mapped to, 217
- Directory functionality, and attribute options, 122
- Directory harvester, and Stanford Directory, 333
- Directory index servers, 168
- Directory information tree, 43, 49
- Directory management, 139–196
 - administrative server parameters, 192–193
 - aliases, 153–155
 - distributed directory, 155–161
 - integrating independent directories, 161–174
 - moving between directories, 174–179

- Directory management, *continued*
 - other tasks for, 193–195
 - referrals, 144–151
 - referral usage, 152–153
 - replication, 140–144
 - and security, 179–193
- Directory namespaces
 - for Active Directory, 231–233
 - divisions for, 54–55
 - flexibility of, 159
- Directory objects, 7
- directoryOperation, 119
- directoryOperation attributes, 127
- Directory operations, representation of in DSML, 178
- Directory root, 23, 24
- Directory security, 196
- Directory Server (Netscape/Sun), 210, 271–310
 - access control instructions and, 358–369
 - Administrator's Guide*, 306
 - documentation with, 275
 - DSML support through, 178
 - flexibility with, 273
 - history behind, 271–272
 - indexes, 279, 357, 358
 - management with, 301–305
 - namespace employed by, 273–282
 - operations and clients with, 282–289
 - platforms supported by, 273
 - plug-ins for, 369–371
 - replication, 302–304
 - schema deployed by, 289–301
 - security with, 305–309
 - strengths of, 309–310
- Directory Server controls, 285–287
 - Manage DSA IT control, 285
 - Persistent Search control, 285
 - Entry Change Notification control, 285
 - Password Expired control, 286
 - Password Expiration Warning control, 286
 - Virtual List View Request control, 286
 - Virtual List View Response control, 286
 - Server Side Sort control, 286
 - Proxy Authorization control, 287
 - Chaining Loop Detection control, 287
- Directory server storage management, 194
- Directory Service Agent, 201
- Directory Service Protocol, 201
- Directory services, DNS and registering of, 47
- Directory Services Markup Language, 30, 178–179, 196, 309
- Directory synchronization, 169–170
- Directory Synchronization (DIRSYNC) control, 96, 173, 314, 352
- Directory System Agent, 201
- Directory Systems Agent Specific Entry container, 32
- Discretionary access control list, 264
- displaySpecifier, 238
- Distinguished names, 24, 60–61
 - and add operation, 87
 - and authentication, 184
 - extended match filter searching for, 82, 83
 - and macros, 308
 - and referral resolution, 145
 - special characters in, 62
- Distributed directory, 33–34, 155–161
 - data architecture for, 162
 - and maintenance, 160–161
 - by multimaster replication in ring topology, 158
 - OpenLDAP and functionality with, 204–205
 - referrals and connection between, 149
 - by region and political division, 156
 - reliability with, 156–157
 - and replication topology, 157, 159–160
 - by single-master replication, 157
- distributedOperation, 119
- DIT. *See* Directory information tree
- DN component, 64
- DNs. *See* Distinguished names
- DNS. *See* Domain Naming System
- DNS extensions, 134
- dNSHostName attribute, 254

DNS records, 194
DNS services, Active Directory integration with, 230–231
DNS SRV records, 273
 AD server located with, 230
 functionality with OpenLDAP, 202
Domain controllers, 232, 233, 236, 241, 253, 256
 and Active Directory replication, 256, 257, 258
 and sites, 235
Domain Controllers container, 242
Domain naming context, 236
Domain Naming Master, 243
Domain Naming System, xvii, 18, 43–47
 and Active Directory, 229–231
 hierarchy in, 44–45
 LDAP and use of, 45–47
 record types in, 45, 46
 resolution, 45
domain object class, 134
Domain partition, in Active Directory, 230, 235, 241–242
Domain tree, 231, 232
Do Not Generate Referrals control, in Active Directory, 354
DSA. *See* Directory System Agent
dSAOperation, 119
dSAOperation operational attributes, 128
DSE container. *See* Directory Systems Agent Specific Entry container
DSML. *See* Directory Services Markup Language
DSP. *See* Directory Service Protocol
DUA. *See* Directory Service Agent
dumpcat, 215
Dynamic authorization, 266
Dynamic groups, and Directory Server schema, 290–291
Dynamic inheritance, 266, 307, 308
dynamicObject object class, 135–136
Dynamic values, dynamic assertion of via Class of Service, 294

E
eDirectory (Novell), 179
EFS. *See* Encrypted File System
E-mail services, and directories, 14, 71
Encrypted File System, 267
Encryption, 35, 36, 39, 180, 181, 185–193, 196
 certificates and certificate authority, 190–191
 digital signatures, 189–190
 and LDAP management, 186
 public key, 187–189
 shared secret key, 186–187
 SSL and TLS, 191–192
Encryption algorithm, 185, 308–309
Encryption settings, with Directory Server, 309
Entries, 38
 dynamic specification of, 362
 elements of auxiliary object class used for creating, 115
 elements of inherited object classes used for creating, 112–114
entry attribute, with OpenLDAP, 214
Entry Change Notification control, 285
Equality matching rule field, in AttributeTypeDescription, 118
Equality matching rules, 323
Equality string match operator (=), 80
Escaping, 62,
Exchange 2000. *See* Microsoft Exchange 2000
extended operation, 28, 29, 94, 97
Extended rights, 239, 265
Extended schema definitions, 134–137
extensibleObject object class, 135, 289, 296
Extensions component in LDAP URL, 64–65
External referrals, 147, 149, 211, 280
F
Family Educational Rights and Privacy Act (FERPA), 165, 331
Filter component, 64

394 Index

Filtered roles, with Directory Server, 292
 Filter operators, 74, 75, 79
 Flat namespaces, 52, 54, 228
 Flexible Single Master Operation, 242, 243
 ForeignSecurityPrincipals container, 242
 Forest, 231, 233, 256
 Forest root domain, 231
 Format string attacks, 63
 FQDN. *See* Fully qualified domain name
 FSMO. *See* Flexible Single Master Operation
 Fully qualified domain name, 254

G

GCs. *See* Global catalogs
 Geographic division, of directory namespace, 54
 Get Security Descriptor control, in Active Directory, 351
 Global catalogs, 169, 240, 244–245, 256
 Globally unique identifiers, 116, 353
 Greater than or equal to string match operator (>=), 80
 GROUPDN, 363
 groupOfURLs class, 290
 Group policy directory entries, 15
 Groups, and Directory Server schema, 290–291
 GUIDs. *See* Globally unique identifiers
 guid attribute, 116
 guidClass, 116

H

Hacking, and LDAP, 63
 Hardcoded programs, and naming attributes, 61
 Harvesting data, 171–174
 Hash function, 189
 Headings, ACI, 307, 360
 Health Insurance Portability and Accountability Act of 1996, 165–166
 Hierarchical namespaces, 42
 HIPAA. *See* Health Insurance Portability and Accountability Act of 1996
 Hub replica, with Directory Server, 302

I

IANA. *See* Internet Assigned Numbers Authority
 IA5string type, 129
 idletimeout directive, 216
 IETF. *See* Internet Engineering Task Force
 Impersonation, 306, 307
 approaches, 220
 features, 219
 Inactive status field
 in AttributeTypeDescription, 118
 in object class definition, 108
 Incremental permissions, 265
 Independent directory integration, 161–174
 and data architecture management, 162–166
 and directory synchronization, 169–170
 and harvesting data, 171–174
 and loose directory interconnection, 170
 and master directory, 167–169
 and metadirectories, 166–167
 Indexes/Indexing
 with Active Directory, 259–260
 with Directory Server, 277, 278–279
 international, 278, 279
 with OpenLDAP, 206–207, 215
 Index servers, 152, 168
 inetOrgPerson object class, 136
 Inheritance
 and access control, 182
 and authorization in Directory Server, 307–308
 auxiliary class *versus*, 117
 building object classes using, 111
 and object class relationships, 110–114
 Inherited permissions, 265
 InitRecvTimeout parameter, 261
 integer type, 129
 Integration
 AD schema and problems with, 251–252
 and data manipulation, 34
 with LDAP protocol, 28
 Interfaces, with Active Directory, 246–247
 Internal structure, of LDAP directory, 48

- International indexing, with Directory Server, 278, 279
 - International language support, 123
 - International Telecommunication Union, 17, 106
 - Internet Assigned Numbers Authority, 131
 - Internet-drafts, 96
 - Internet Engineering Task Force, 17, 203
 - RFCs on Web site of, 19
 - Inter-Site Transports container, 240
 - iPlanet, dissolution of, 272
 - iPlanet Console, 283, 301
 - iPlanet Delegated Administrator, 283, 301
 - iPlanet Directory Server, 266, 271, 272
 - iPlanet MetaDirectory, 302
 - IP restrictions, 193
 - ITU. *See* International Telecommunication Union
- J**
- Java, 100
 - object schema, 136
 - SDKs for LDAP API in, 284
- K**
- KDCs. *See* Key distribution centers
 - Kerberos, 35, 36, 181, 187, 217, 229, 254, 262–263, 328
 - and Microsoft, 263
 - Key distribution centers, 263
 - Keys
 - in database technology, 11
 - encryption and lengths of, 185–186
 - private, 187
 - public, 187
 - secret, 186–187
- L**
- Language support, 123–126
 - Language tags, 207, 208, 213
 - Lazy Commit control, in Active Directory, 352
 - LCUP. *See* LDAP Client Update Protocol, 314
 - LDAP. *See* Lightweight Directory Access Protocol
 - LDAP API functions, 314–316
 - C API, 97, 314–316
 - ldap_abandon, 209, 315
 - ldap_add() function, 27, 99, 315
 - ldap_bind, 209, 315
 - ldap_compare, 209, 315
 - ldapdelete, 209, 283, 315
 - ldap_first_attribute(), 100, 315
 - ldap_first_entry(), 99, 315
 - ldapmodify, 209, 283, 315
 - ldapmodrdn, 209, 315
 - ldap_next_attribute(), 100, 316
 - ldap_next_entry(), 100, 315
 - ldapsearch, 209, 283, 315
 - Netscape SDK, 100
 - PerLDAP SDK, 100
 - in Windows Software Development Kit, 248
 - LDAP client options, 73, 97–98
 - LDAP Client Update Protocol, 96, 314
 - LDAP controls, 78, 94–96, 173
 - and Active Directory, 246, 248–249, 351–355
 - ASQ control, 355
 - Change Notification (Psearch) control, 352
 - Cross Domain Move control, 353
 - Directory Synchronization (Dirsync) control, 352–353
 - Get Security Descriptor control, 351
 - Lazy Commit control, 352
 - Paged Search control, 351
 - Permissive Modify control, 354–355
 - Return Extended DN control, 353
 - Search with Local Scope control, 354
 - Server Search Operations control, 354
 - Show Deleted Objects control, 352
 - Sorted Search Request control, 352
 - Sorted Search Response control, 354
 - Statistics control, 353–354
 - Tree Delete control, 353
 - Verify Server Name control, 354

396 Index

LDAP controls, *continued*

- Virtual List View Request control, 355
- Virtual List View Response control, 355
- and Directory Server, 285–287
 - Manage DSA IT control, 285
 - Persistent Search control, 285
 - Entry Change Notification control, 285
 - Password Expired control, 286
 - Password Expiration Warning control, 286
 - Virtual List View Request control, 286
 - Virtual List View Response control, 286
 - Server Side Sort control, 286
 - Proxy Authorization control, 287
 - Chaining Loop Detection control, 287
- Draft Controls, 313–314
 - Change Notification (PSEARCH) control, 250, 313
 - Triggered Search (TSEARCH) control, 313
 - Directory Synchronization (DIRSYNC) control, 96, 173, 314, 352
- and OpenLDAP, 210–211
 - Manage DSA IT control, 204, 210
 - Password modify control, 208
- Standardized controls
 - Paged Search control, 95
 - Server Side Sort control, 95
- LDAP Data Interchange Format, 34, 174–177, 195, 255, 275
 - entry with folding and encoding in both base64 and UTF-8, 176
 - examples with, 176–177
 - standard for, 175
- LDAP_DEREF_*, 97
- LDAP directories
 - example of naming contexts in, 53
 - flat namespace in, 54
 - invalid hierarchical namespaces in, 58
 - and LDAP controls, 94
 - and LDAP schema, 103
 - security for, 179–193
 - valid hierarchical namespaces in, 50
 - X.500 directories *versus*, 282
- LDAP directory products, 37
- LDAP discussion mailing lists, OpenLDAP
 - hosting of, 208
- LDAP-enabled application, 27
- LDAPMessage, 99
- LDAP namespaces, 41–67
 - advantages with, 25–26, 48
- LDAP object structure, 48–53
- LDAP operations, 85–93
 - abandon, 93
 - and access control rights, 182
 - add, 87–88
 - bind, 86
 - compare, 86–87
 - delete, 88
 - LDIF format used for requesting, 175
 - modify, 88–89
 - modify RDN, 89–92
 - schema modifications via, 110
 - search, 73–76, 86
 - unbind, 93
- LDAP_OPT_*, 97–98
- LDAP proxy, with Sun Directory Proxy Server, 301
- LDAP schema, 103–138
 - and attributes, 117–129
 - checking, 132–133
 - conceptual diagram of, 104
 - documents defining, 105
 - extended schema definitions, 134–137
 - matching rules, 130–131
 - modifying, 103–104
 - and object classes, 107–117
 - OIDs, 131–132
 - syntaxes, 129–130
 - turning off, 133
 - X.500 and affect on, 106
- LDAP schema Internet drafts, 137
- LDAP_SIZELIMIT_EXCEEDED, 78, 79
- ldapSyntaxes attribute, 130
- LDAPURL, 363

- LDAP URL format, and referrals, 148
 - LDAP v2
 - Active Directory support for, 245
 - lack of support for referrals with, 144, 145
 - LDAP v3 contrasted with, 66
 - naming conventions in, 65–66
 - LDAP v3, 99
 - Active Directory compliance with, 245 and ADSI, 248
 - Directory Server compliant with, 282
 - extended match filters with, 81
 - LDAP v2 contrasted with, 66
 - operational attributes and, 126
 - referrals with, 144, 145
 - and schema, 107
 - security warnings with, 179
 - Unicode Transformation Format–8 used by, 123
 - LDAPv3 Triggered Search Control, 313
 - LDBM
 - database type, 206
 - and Directory Server, 274, 277
 - indexing directives for, 207
 - LDIF. *See* LDAP Data Interchange Format
 - LDIFDE, 255–256
 - LDIF export, via slapcat, 215
 - LDIF files, and Directory Server schema, 289
 - LDIF import, via slapadd, 214
 - ldp.exe, 261
 - Less than or equal to string match operator (<=), 80
 - Lightweight Directory Access Protocol, xvii, xix, 100–101, 271
 - advantages summary, 38–40
 - APIs, 98–100
 - connectionless, 85
 - master directories with support for, 167
 - Mycompany.com
 - applications/infrastructure integrated with, 20
 - namespaces, 21–26
 - naming contexts, 52–53
 - object naming, 56–60
 - overview of, 3–40
 - reasons for choosing, 37–40
 - schema, 30–32
 - special structural concepts, 67
 - structure rules, 51–52
 - Link Bridge entries, 240
 - Linked attributes, 254–255
 - Link entries, 240
 - Load balancing, with distributed directories, 33, 159
 - loglevel directive, 216
 - Loop Detection control, 281
 - Loose directory interconnection, 170, 171, 336
 - Loosely synchronized partition, 143
 - LostAndFound container, 239, 242
- M**
- Macros, and ACIs, 308, 368–369
 - Macro variables, methods supporting, 368
 - Managed roles, with Directory Server, 292
 - Manage DSA IT control, 204, 210–211, 285
 - manager attribute, 301
 - Mandatory attributes field, in object class definition, 109
 - Master directories, 167–169
 - Master replica, with Directory Server, 302
 - Match filters, extended, 81–83
 - Matching rule definitions, 130–131
 - Matching rules, 124, 130–131, 138, 322–325
 - and attributes, 117
 - common usage of in LDAP schema definitions, 322, 323
 - and language support, 125
 - and LDAP schema, 104, 105
 - list of common matching rules, 322–325
 - and OpenLDAP, 212
 - MatchingRuleUse attribute, 130
 - Matching rule use definitions, 130–131
 - Matching Rule Use Description syntax, 131
 - Match operators, 79, 80–81
 - MaxActiveQueries parameter, 261
 - MaxConnections parameter, 261
 - MaxConnIdleTime parameter, 261

398 Index

MaxNotificationsPerConn parameter, 261
 MaxPageSize parameter, 261
 MaxPoolThreads parameter, 262
 MaxQueryDuration parameter, 262
 MaxResultSetSize parameter, 262
 MaxTempTableSize parameter, 262
 may attribute/field, 109–110
 mayContain attribute, 253
 Message digest, 189
 Messaging Direct, 85
 Metadirectories, 161, 166–167
 Microsoft, 96. *See also* Active Directory (Microsoft)
 and Active Directory adoption, 267–28
 Address Book with, 246
 ADSI SDK, 100
 certificate authority server software, 266
 and directory products, 269
 DSML support through, 178
 and Kerberos standard, 263
 Microsoft Exchange 5.5, 249
 Microsoft Exchange 2000, 71, 244, 249–251
 Microsoft Management Console, 238, 255, 268
 Microsoft Metadirectory Services, 255, 260
 Microsoft Windows Software Development Kit, 248
 MMC. *See* Microsoft Management Console
 MMS. *See* Microsoft Metadirectory Services
 Modifiable field, in
 AttributeTypeDescription, 119
 modifiersName, 213
 modify DN operation, for modifying only the RDN, 90
 modify operation, 88–89, 105, 154
 modify RDN operation, 29, 30, 89–92, 105
 for modifying both RDN and moving the entry, 91
 for modifying RDN, while leaving old RDN, 92
 parameters for, 93
 modifyTimestamp, 213

Multimaster replication, 142, 143
 with Active Directory, 255, 256
 distributed directory by, in ring topology, 158
 single–master replication model *versus* , 143
 Multiple–class inheritance, OpenLDAP support for, 212
 Multiple–language directories, 124
 Multiple–master replication, with Directory Server, 303
 Multivalued attributes, 117
 Multivalued RDN, example of, 59
 must attribute/field, 109, 110
 mustContain attribute, 253

N

Name field
 in AttributeTypeDescription, 118
 in object class definition, 108
 Name form, in object class definition, 105
 Names, attribute, 119–120
 Namespaces
 Active Directory, 228–245
 directory, 21–26
 Directory Server, 273–282
 LDAP, 41–67
 OpenLDAP, 202–207
 postal example of, 42
 Naming attribute field, 109
 Naming attributes, 57, 58–60
 appropriate use of, 61–62
 common attributes used as, 58
 Naming contexts, 52–55, 140
 with Active Directory, 236
 with Directory Server, 274–277
 and distributed directories, 159
 with OpenLDAP, 203
 and replicas, 141
 Naming conventions, LDAP v2, 65–66
 NDS. *See* Novell Directory Services
 Nested groups, 290
 Nested roles, with Directory Server, 292
 Netbios, 228–230
 note on turning off, 229

- Netscape, xviii, 96, 278. *See also* Directory Server
 LDAP SDK, 100
 server products from, 283
 Sun *versus*, 272
- Netscape Calendar Server, 284
- Netscape Certificate Management System, 284
- Netscape Certificate Server, 284
- Netscape Communicator browser, and Directory Server, 283
- .NET Server 2003, 236, 237, 248, 251, 252, 269
- Network operating systems
 and directories, 14, 15
 and vendor LDAP products, 37
- Network World, 272
- neverDerefAliases, 78
- Noncontiguous DNS zones, Active Directory support for, 231
- NOSs. *See* Network operating systems
- NOT operator (!), 75
- Novell Directory Services, 246, 248
- nsds5ReplConflict attribute, 303
- nsFarmServerURL attribute, 282
- nsFilteredRoleDefinition object class, 292
- nsHopLimit attribute, 281, 287
- nsManagedRoleDefinition object class, 292
- nsMatchingRule, 278
- nsMultiplexorBindDN attribute, 282
- nsMultiplexorCredentials attribute, 282
- nsNestedRoleDefinition object class, 292
- nsRole attribute, 291
- nsRoleDN attribute, 291, 292, 293
- nsslapd-backend attribute, 277
- nsSlapdPlugin object class, 289
- nss-lapd-referral attribute, 282
- nsslapd-state attribute, 277
- nsSystemIndex value, 278
- nsuniqueid attribute, 303
- NTLM authentication, 262
- nTSecurityDescriptor attribute, 264–266, 351
- O**
- Objectclass, difference between Object class and, 9
- objectClass attribute, 8, 107, 112, 128
- Object classes, 107–117, 138
 categories of, 107
 and containers, 57
 definition, 104
 elements of, 108–110
 and entry creation, 110–117
 inheritance, 110–114
 and LDAP schema, 104
 structure rules, 51–52
- objectGUID attribute, 253
- Object identifiers, 57, 77, 131–132
 and extended match operators, 82
 creating Arcs, 131
 in AttributeTypeDescription, 118
 in object class definition, 108
 problems with, 132
- Object naming, LDAP, 56–60
- objectSID attribute, 253
- OBSOLETE, 108
- Octet strings, 129
- OIDs. *See* Object identifiers
- 1.1 attribute, 77
- One scope, 74
- OpenLDAP, 199–225, 277, 335
 advantages/disadvantages with, 223–225
Administration Guide, 343
 design flexibility with, 213
 indexes, 206–207
 ManageDsaIT control supported by, 210
 management tools with, 214–216
 namespace, 202–207
 operations and clients with, 208–209
 replication, 205
 schema deployed by, 211–214
 security with, 216–223, 341–348
 special configuration parameters with, 215–216
 strengths of, 223–225

400 Index

OpenLDAP access control, 341–348
 <access> element, 344–345
 comprehensive example for,
 346–348
 <what> element, 341–342
 <who> element, 342–344
OpenLDAP schema, 211–213
 attributes, 213
 classes, 212–213
 default schema definitions, 211
OpenLDAP security, 216–223
 authentication, 216–220
 authorization, 221–223
 privacy, 223–225
Open source, 199
 APIs, 27
 closed source or?, 200
 movement, 37
OpenSSL, 223,
operatingSystem attribute, 254
operatingSystemHotfix attribute, 254
operatingSystemVersion attribute, 254
Operational attributes, 77, 126–129
 in Active Directory classes, 253
 OpenLDAP support for, 213
operational value, 119
Operations, 28, 40
Operators, in LDAP schema, 31
Optional attributes field, in object class
 definition, 109
Optional parameters, 79
Optional search parameters, 77–79
Ordering matching rules, 325
Order matching rule field, in
 AttributeTypeDescription, 118
Organizational units, 266
Organization Registry, in Stanford Registry,
 330
OR operator, 75
Orphaned entries, 239
ou class, 9
OUs. *See* Organizational units
Ownership, of data, 162, 163

P

Paged Search control, 95, 351
Parameters
 for abandon operation, 93
 for administrative server, 192–193
 for bind operation, 86
 for compare operation, 87
 for delete operation, 88
 for modify operation, 88–89
 for modifyRDN operation, 93
 optional, 79
Parent/child relationships, and containers,
 9, 49
Parentheses, and regular expressions, 218
Parent zones, 44
Partitions, 140–141, 195
 with Active Directory, 236–244 256
 example of, 142
 with OpenLDAP, 203
Partitions container, 239
Pass thru authentication, 306, 310
Password Expiration Warning control, 286
Password Expired control, 286
Password modify control, 208
Password modify extended operation, 94
Passwords, 14
 and authentication, 180, 181
 and directories, 14
 and Directory Server authentication,
 305–306
PDC Emulator Master, 243
People-friendly directories, designing, 66
Performance
 with Directory Server, 309
 monitoring, 195
Period character, and regular expressions, 218
Permissions
 ACI, 259, 307, 360
 in Active Directory, 264
 incremental, 265
Permissive Modify control, in Active
 Directory, 354
Persistent Search control, 96, 285

- Person entries, 7–8
 - Person object class, sample schema definition for, 32
 - Phone numbers, attributes and, 60
 - Pine e-mail program, 77
 - PKI. *See* Public key infrastructure
 - Plug-ins, 282, 287–289, 369–371
 - and chaining, 280, 281
 - Pass Thru Authentication, 306
 - Policies container, 260
 - Political/functional division, of directory namespace, 54
 - Portals, 28
 - possSuperiors attribute, 252
 - postalAddress value, 296, 297, 299
 - Privacy, 35, 36, 163. *See also* Security
 - with Active Directory, 262, 266–267
 - of data, 163, 165
 - with Director Server, 308–309
 - and encryption, 185
 - in Stanford Registry, 331, 332–333
 - in Stanford’s Active Directory, 338–339
 - Private keys, 187
 - Programming support
 - with Active Directory, 248
 - with Directory Server, 284
 - with OpenLDAP, 209–210
 - Propagation dampening, 257
 - Property. *See* Attribute.
 - Proxy, 170, 171
 - Proxy authorization, 285, 306
 - Proxy Authorization control, 287, 306
 - ProxyDN, 307
 - Proxy shadow accounts, 262
 - PSEARCH, 96, 173, 313
 - PTA. *See* Pass thru authentication
 - Public key certificate, 36, 266–267
 - Public key encryption, 187–189, 188, 191, 192
 - Public key infrastructure, 186, 196, 262
 - Public keys, 187
 - Public–private key authentication methods, 181
- Q**
- Query operations, 28, 29
 - Quotation marks, and search filter items, 74
- R**
- RDN. *See* Relative distinguished name
 - Read-only servers, and single-master replication models, 144
 - Recipient Update Service, 250
 - Red Hat Linux distribution, OpenLDAP with, 224
 - Referential Integrity plug-in, 293, 303
 - Referral chaining parameter, 193
 - Referral loops, 145, 152
 - Referrals, 30, 67, 139, 144–153, 146
 - in Active Directory topology, 240
 - aliases *versus*, 153, 154
 - chaining, 151
 - with Directory Server, 280
 - distributed directories connected by, 149
 - examples of, 149–151
 - and master directories, 167
 - and OpenLDAP, 204
 - resolution, 145–148
 - syntax, 148
 - usage of, 152–153
 - referral value, 277
 - ref object class, 213
 - Regular Expressions (regex), 218
 - Relative distinguished name, 24, 56–58, 82
 - and add operation, 87
 - example of, 57
 - multivalued, 59
 - and naming attributes, 58
 - Reliability, with distributed directory, 156–157
 - Replicas, 141–144
 - example of, 142
 - Replication, 33, 43, 67, 139, 140–144, 195
 - with Active Directory, 256–259, 268
 - with Directory Server, 277, 290, 302–304
 - harvesting *versus*, 171, 173

402 Index

- Replication, *continued*
 - partitions, 140–141
 - replicas, 141–143
 - between sites, 235
 - troubleshooting, 195
 - Replication agreements, 302
 - Replication Manager entry, 303
 - Replication topology
 - with Active Directory, 237
 - for distributed directories, 157, 158, 159–160
 - repllogfile directive, 205
 - Result codes, 84–85
 - Retro Change plug-in, 303
 - Return Extended DN control, in Active Directory, 353
 - rfc822MailGroup, 209
 - RID Master FSMO role, 243, 253
 - Ring topology
 - for AD multimaster replication, 256, 257
 - distributed directory by multimaster replication in, 158
 - for limiting replication connections, 142
 - ROLEDN, 363
 - Role entries, 291–293
 - Root, of directory, 23
 - rootdn entry, 223
 - Root domain, in Active Directory forest, 231, 236
 - Root DSE, 32, 52, 94, 126, 128
 - Root namespace service, with OpenLDAP, 203
 - rootpw directive, 223
 - Root zones, 44
 - RUS. *See* Recipient Update Service
- S**
- SAM. *See* Security Accounts Manager
 - sAMAccountName attribute, 253
 - SASL. *See* Simple Authentication and Security Layer
 - saslAuthzFrom attribute, 219
 - saslAuthzTo attribute, 219
 - saslRegexp directives, 217
 - Scalability, 53–55, 145
 - Schema checking, 31, 105, 132–133
 - Schema definitions
 - chaining via, 280
 - extended, 134–137
 - and inheritance, 112
 - Schema extensions, 31–32
 - Schema formats, 119, 317–320
 - ASN.1 syntax, 318
 - BNF syntax, 318–319
 - slapd.conf syntax, 319
 - Schema maintenance, 194
 - Schema Master, with Active Directory, 243
 - Schema naming context, with Active Directory, 236
 - Schema partition, with Active Directory, 243–244
 - Schema(s), 8, 30–31, 40
 - Active Directory, 251–255
 - common syntaxes for, 320, 321–322
 - Directory Server, 289–301
 - LDAP, 103–138
 - OpenLDAP, 211–213
 - syntaxes, 31–32
 - Schema violations, and operation failure, 133
 - scope, of search, 74
 - Scope component, 64
 - SDKs. *See* Software Development Kits
 - Search Assistant, 247
 - Search filter items, 74
 - Search filters, 74, 77, 79–83
 - extended match operators specified in, 82
 - operators, Mycompany example for, 76
 - and referrals, 146
 - special characters in, 83
 - search operation, 29, 73–76, , 79, 86
 - Search parameters, 73
 - mandatory, 73–74
 - optional, 77–79
 - Search query limit, 193
 - Search with Local Scope control, in Active Directory, 354
 - Secret key encryption, 192

- Secure Sockets Layer, 35, 36, 186, 191–193, 308
- Security, 34–36
 - with Active Directory, 255, 262–267
 - with Directory Server, 305–309, 310
 - of distributed directory servers, 160
 - with OpenLDAP, 216–223, 224
- Security Accounts Manager, 248
- Security for directories, 179–193
 - authentication, 180–182
 - authorization, 182–185
 - encryption, 185–191
 - SSL and TLS, 191–192
- Semicolons (;)
 - add operation requests, 88
 - and attribute option specification, 123
- sendmail, 71
- Server Search Operations control, in Active Directory, 354
- Server-side referral handling, 153
- Server Side Sort control, 95, 286
- Server-to-server interactions, and LDAP directories, 101
- Service interruptions, with OpenLDAP, 222, 223, 224
- servicePrincipalName attribute, 254
- Services container, 240
- Session encryption, 94, 208
- Session timeout parameter, 193
- Shared secret key encryption, 186–187
- Show Deleted Objects control, in Active Directory, 352
- Simple Authentication and Security Layer, 35, 216, 262, 305
- Simple LDAP Change Notification Mechanism, 313
- Simple Object Access Protocol, 178
- Single-master replication, 141
 - distributed directory by, 157
 - multimaster replication model *versus*, 143
 - slurpd process and support for, 205
- Sites, 236, 240
 - Active Directory, 234–236, 256
 - advantages with, 237
 - domains distributed across, 235
 - sizeLimit, 78, 95, 216
 - slapadd program, 214, 215
 - slapcat program, 215
 - slapd.conf schema format, 319
 - slapd configuration, and replication behavior, 205
 - slapd configuration file (slapd.conf), 215, 217
 - example, 346–348
 - schema definitions in, 211
 - slapd process, with OpenLDAP, 201, 214
 - slapindex, 215
 - slurpd process
 - with OpenLDAP, 201–202
 - single-master replication supported via, 205
 - Smart cards, with Active Directory, 263
 - Smart referrals, 280
 - sn attribute, 113
 - SOAP. *See* Simple Object Access Protocol
 - Software Development Kits, 248, 284, *also see* LDAP API functions
 - Sorted Search Request control, 352
 - Sorted Search Response control, 286, 354
 - Source, of data, 162
 - Special characters, 66
 - in distinguished names, 62
 - in search filters, 83
 - Special configuration parameters, with Directory Server, 304–305
 - Special search filter characters, 83
 - Special URL characters, 65
 - SQL, and OpenLDAP, 206
 - SSL. *See* Secure Sockets Layer
 - Stanford Directory, 333, 334–336
 - e-mail service integration in, 335
 - personal information updates in, 336
 - Web UI integration in, 335
 - Event database and harvester, 334
 - Stanford Registry, 328–331
 - Stanford University directory architecture, 327–339
 - Active Directory harvester, 336–338
 - directory harvester, 333–334
 - environment, 327–328

404 Index

Stanford University directory architecture,
continued
source systems, 328, 329
Stanford Directory, 334–336
Stanford Registry, 328–333
Windows Infrastructure, 333, 336
Stanford.You, 336
Static groups, and Directory Server schema,
290–291
Static inheritance, 307, 308
Statistics control, 248, 353–354
String match operators, 80
Structural classes, 107, 114
Structure, 49
and containers, 10
of directories, 6, 55–56
and namespace, 41
Structure rules, in object class definition,
104–105
Subordinate entry to container, 49
Subordinate referrals, 147, 149, 204
subschema entry, 109, 128, 325
subschemaSubentry, 107, 213, 244
Subscribers, and data, 164
Substring matching rules, 118, 325
Substring values, wildcards used for
matching, 80
Subtree scope, 74, 75
Subtree search filters, 362
Suffixes, language code, 124
Suffix referrals, 280
Sun, 274, 278, 309. *See also* Directory
Server
Netscape *versus*, 272
online documentation site for, 301
server products from, 283
Sun Directory Proxy Server, 284, 301
Sun–Netscape Alliance, 271
Sun ONE Calendar Server, 284
Sun ONE Identity Server, 274
Sun ONE Messaging Server, 284
Sun Portal Server, 284
Superior classes, 108, 111, 112
Superior class field, in
AttributeTypeDescription, 111, 118

Superior referrals, 147, 204
Superior rules field, 109
supportedControl attribute, 95
surname (sn) attribute, 252
Synchronization, directory, 169–170
Synchronous versions, for API functions, 99
Synonyms, attribute name, 119, 120
Syntax(es), 31–32, 46, 104, 105, 129–130,
138, 320, 321–322
ACIs, 308
for Active Directory, 252
for add operation requests, 88
for attribute values, 117
for extended match filter, 82
and language support, 125
for LDAP URL, 63–65, 148
list of common syntaxes, 320–322
for OpenLDAP, 212, 214, 215
and plug-ins, 287–288
for search filter item, 74
for subtypes, 120
Syntax field, in AttributeTypeDescription,
118
System container, 242
systemMayContain attribute, 253
systemMustContain attribute, 253
systemPossSuperiors attributes, 252

T

Ticket granting ticket (TGT), 337
TimeLimit, 79
Timestamps, 258, 259, 303
TLS. *See* Transport Layer Security
Tombstone, 257, 258
top class, 114, 253, 296
Transport Layer Security, 35, 36, 180, 186,
192, 223
Directory Server support for, 308
session encryption via, 208
Tree, 231
Tree Delete control, in Active Directory,
353
Tree structure, 49
TSEARCH, 96, 173, 313
TypesOnly, 79

U

UDP transactions, and CLDAP basis, 86
Unbind operation, 29, 93
Unicode Transformation Format–8, 30, 39, 123, 125
University of Michigan, 17, 271
University of Michigan code, 200, 201
Update sequence number, 258
URL naming, 63–65
Usage field, in AttributeTypeDescription, 119
userApplications, 119, 126
userCertificate attribute, 254, 306
User classification division, of directory namespace, 55
USERDN, 363
User entries, in Active Directory, 253
User object class, 253, 254
userPrincipalName attribute, 253
Users container, 242
USN. *See* Update sequence number
UTF–8. *See* Unicode Transformation Format–8

V

Vendors, 37–38
Verify Server Name control, in Active Directory, 354
Verisign, 190
Virtual list view, 96, 278, 279, 314
 Virtual List View Request control, 286, 355
 Virtual List View Response control, 286, 355
Visibility attributes, in Stanford Registry, 332
vlindex command, 279

W

Web–based client interface, 72–76
Web sites, LDAP–enabled, 28

WellKnownSecurityPrincipals container, 240
What attribute information to return search parameter, 77
<what> element, 341–342, 345
<who> element, 345
Wildcards, 363
 and ACI bind rules, 361
 example, 81
 and macros, 308
 for matching substring values, 80
Windows platform, LDAP programming support from, 246
Windows Software Development Kit. *See* Microsoft Windows Software Development Kit
WMI, 249
Workgroup Registry, in Stanford Registry, 331

X

X.209, 129
X.500, xvii, 17, 137, 253
 and aliases, 153
 and chaining, 153
 and Directory System Agent, 201
 LDAP directories *versus*, 282
 and LDAP schema, 31, 106
 master directories with support for, 167
 naming style, 273
 online references, 19
 problems with, 18
 subtypes in, 120
X.509 certificates, 36, 129
XML, 30, 178

Z

Zones, 44