

Index

- : (colon), in DNs, 93–96
- () (parentheses), grouping search terms, 78
- & (ampersand), AND operator within search filters, 78
- * (asterisk), wildcard within search filters, 73–74
- = (equal sign)
 - equality operator within search filters, 74
 - in multivalued RDNs, 66
- ! (exclamation point), negation within search filters, 78
- <= (left angle, equal sign), greater than or equal to operator within search filters, 75
- + (plus sign), in search operations, 73
- # (pound sign), comment indicator, 783
- >= (right angle, equal sign), greater than or equal to operator within search filters, 75
- | (vertical bar), OR operator within search filters, 78
- ~= (tilde, equal sign)
 - approximation operator within search filters, 74–75
- 2222 (*SASL...*) RFC, 139
- 2251 (*LDAPv3*) RFC, 47
- 2252 (*LDAPv3 Attribute Syntax Definitions*) RFC, 47, 61–62, 274
- 2253 (*LDAPv3 UTF-8 String Representation of Distinguished Names*) RFC, 47
- 2254 (*String Representation of LDAP Search Filters*) RFC, 47
- 2255 (*LDAP URL Format*) RFC, 48
- 2256 (*Summary of the X.500(96) User Schema for Use with LDAPv3*) RFC, 48
- 2587 (*Internet X.509 Public Key Infrastructure LDAPv2 Schema*) RFC, 290
- 2820 (*Access Control Requirements for LDAP*) RFC, 142
- 2829 (*Authentication Methods for LDAP*) RFC, 48, 90, 125
- 2830 (*Extension for Transport Layer Security*) RFC, 48, 92–93
- 2830 (*[LDAPv3] Extension for Transport Layer Security*) RFC, 142
- 2831 (*Using Digest Authentication as a SASL Mechanism*) RFC, 140
- 2891 (*LDAP...Sorting of Search Results*) RFC, 131
- 3377 (*LDAPv3: Technical Specification*) RFC, 48
- abandon operation, 56, 87–88
- abstract object classes, 268
- Access, Searching, and Indexing of Directories (ASID)
 - IETF working group, 49
- access control
 - application needs definition, 219
 - applications for, 654–657
 - data design, 239
 - definition, 90
 - delegation, case study, 867–871
 - in the hands of users, 841
 - information, backup and restore, 542
 - models, 91
 - namespace design, 311
 - Netscape Directory Server, 167–173
 - replication, 396
 - security design, 432–434
- access control instructions (ACIs), 167, 169–173
- access control lists (ACLs). *See* ACLs (access control lists).
- access control policy, 433–434
- Access Control Requirements for LDAP* (RFC 2820), 142
- ACIs (access control instructions), 167, 169–173
- ACLs (access control lists)
 - description, 432–433
 - examples, 434–438
 - placement, 439–440
 - replication, 396
- actionPerformed() method, 752
- Active Directory, 345, 394
- Active Directory Services Interface (ADSI) API, 118
- add changetype LDIF statement, 96–97
- add modifytype LDIF statement, 97
- adding
 - ACIs (access control instructions), 169–171
 - auxiliary information to directory entries. *See* auxiliary classes.
 - directory entries
 - add operation, 56, 82
 - ldapmodify utility, 111–112
 - LDIF, 96–97
 - schemas to directory servers, 289–290

880 Index

- address book applications, 356
- administrators. *See* system administrators.
- ADSI (Active Directory Services Interface) API, 118
- aggregating servers, 368
- AIM Enterprise Gateway, 177
- alias dereferencing, 72
- aliases, 68–69
- allowed (optional) attributes, 268, 274–277
- Alvestrand, Harald, 292
- American Standards Institute (ANSI), 292
- ampersand (&), AND operator within search filters, 78
- analyzing
 - data elements, 251
 - environment
 - application software, 215
 - coexistence with other systems, 228
 - computer systems, 213–214
 - criticality of service, 228
 - hardware constraints, 227
 - network constraints, 227–228
 - networks, 214–215
 - organizational structure and geography, 213
 - overview, 210, 211–212
 - prioritizing constraints, 228–229
 - security constraints, 228
 - software constraints, 227
 - log files, 410, 580–581, 590–591
- AND operators within search filters, 78
- Andresen, Marc, 798
- anonymous bind (authentication), 102–103, 427–428
- anonymous users, 427–428
- ANSI (American Standards Institute), 292
- AOL Instant Messenger (AIM), 177, 179, 738
- AOL Time Warner, 821
- APIs
 - ADSI (Active Directory Services Interface), 118, 662
 - C language, 116–117, 658
 - Java, 117, 658, 662
 - JNDI (Java Naming and Directory Interface), 118, 662, 693
 - online resources, 115–116, 117–118
 - Perl, 117, 659
 - Python, 117, 659
 - SDKs, sources for, 115–116
- application-maintained data, 560–562
- application needs
 - access control, 219
 - auditing, 219
 - authentication, 219
 - data, 216–217
 - level of service, 218
 - overview, 211
 - performance, 217–218
 - prioritizing, 219–220
 - privacy, 219
 - security, 219
 - versus* user needs and expectations, 223
- application-specific directories, 6, 761–762
- applications
 - as data source, 254
 - developing. *See* developing applications.
 - namespace design considerations, 312, 320–321
 - needs definition, 215
- arcs, for OIDs 77, 292
- ASID (Access, Searching, and Indexing of Directories)
 - IETF working group, 49
- ASN.1 schema format, 280–283
- asterisk (*), wildcard within search filters, 73–74
- attribute types. *See* attributes.
- attribute values, 60–62, 95–96. *See also* data, element values.
- attributes
 - case sensitivity, 262
 - definition, 33
 - description, 60–62
 - designing schemas
 - allowed (optional), 268, 274–277
 - hierarchies, 264–265
 - matching rules, 265, 267
 - naming, 262, 291
 - operational, 263
 - subtypes, 264–265
 - supertypes, 264–265
 - syntax, 265, 266
 - type example, 263–264
 - usage indicators, 262, 276
 - values, 262
 - mandatory, 268
 - usage indicators, 262, 276
- attributeTypes attribute type, 274–277
- auditing, 219, 417
- authentication. *See also* security.
 - application needs definition, 219
 - certificate-based client, distributed directories, 350
 - credentials, verifying, 650–652
 - data maintenance, 567
 - definition, 10, 88
 - designing, 427–431
 - distributed directories, 348–351
 - LDAPv3 methods, 90
 - process of. *See* binding.
 - simple, 88
 - tools for, 417, 418
- authentication and control operations, 56, 86–88
- authentication applications, 356
- authentication database, 35
- Authentication Methods for LDAP* (RFC 2829), 48, 90, 125
- authorization, proxied, 136–137, 167–173
- auxiliary classes, 268, 279, 295–297
- availability, 17–18, 248, 331, 358, 398, 504,
- backdoor access, 413
- backup and restore. *See also* disaster recovery.
 - access control information, 542
 - case studies, 815, 846, 874
 - causes of, 538
 - change history, 542

- cost, 514–515
- databases, 164–165
- directories *versus* file systems, 538
- directory server configuration files, 542
- incremental backups, 539
- LDIF backup and restore, 540–542
- Netscape Directory Server, 540, 543
- online directory servers, 539
- with replication, 543–545
 - restoring databases, 165–167
 - safeguarding backups, 545, 548
 - schema configuration files, 542
 - single-master replication, 546–547
 - snapshot restores, 540
 - verifying backups, 548–549
- bak2db command, 165–167
- bak2db script, 540
- base-64 encoding, 95–96
- Basic Encoding Rules (BER), 59
- batch updates, as data source, 256–257
- BER (Basic Encoding Rules), 59
- bind operation, 56, 86–87
- binding, 89, 102–103
- British Standards Institute (BSI), 292
- browsing *versus* searching, 25
- BSI. *See* British Standards Institute.
- Bulk Import Finished extended operation, 138–139
- Bulk Import Start extended operation, 138–139
- bulk loading databases, 161

- C language API, 116–117, 658
- C language SDK, 115–116, 658
- The C LDAP Application Program Interface*, 142
- cascaded replication configuration, 403
- case studies. *See* enterprise with an extranet; examples; large multinational enterprise; Netscape Communications Corporation.
- centrally maintained data, 563–565
- certificate authority, 444
- certificate-based client authentication, 350
- certificates
 - authentication, 430–431
 - issuance, 444
 - life cycle management, 31, 652
 - location problem, 31
 - revocation list, 445
- chaining, 343–344
- change control policy, 638
- change history, 542
- change sequence numbers (CSNs), 379
- changelog, 379
- chasing referrals, 342, 381, 670
- choosing an overall approach, 212, 229–230
- choosing directory services software. *See* evaluating directory services software.
- Clark, Jim, 798
- class of service (CoS) feature, 179
- `clearSessionValues()` method, 708
- client replication updates *versus* replica updates, 387
- client use of LDAP, 54–56
- clock synchronization, 385–386
- coexistence
 - common data sources, 761–763
 - copying to/from data sources
 - migration, 763–764
 - N-way join, 768–770, 783–793
 - one-way synchronization, 764–766, 783–793
 - two-way synchronization, 766–768
 - virtual synchronization, 770–773
 - data source security, 776
 - data translation, 772–774
 - data transport, 775–776
 - designing for, 228
 - implementation considerations, 780–783
 - importance of, 761–763
 - monitoring, 782–783
 - new applications, 663–665
 - overview, 759–761
 - performance considerations, 781
 - requirements definition, 777–780
 - security and privacy considerations, 774–776
 - tools for, 781–782
 - troubleshooting, 782
 - tuning, 782
 - unique join attributes, 775
- coexistence tables, 779
- cold-site recovery, 552–554
- colon (:), in DNs, 93–96
- combining data from multiple sources. *See* joins.
- command-line utilities
 - `ldapmodify`, 110–115, 569
 - `ldapsearch`
 - binding, 102–103
 - definition, 101
 - encrypting server communications, 105–106
 - filters, 102, 104–105
 - options, 106–110
 - retrieving a single entry, 102
 - retrieving specified attributes, 103–104
 - sample searches, 101–102
 - search base, 102
 - searching with SSL (Secure Sockets Layer), 105–106
 - online sources for, 127
- compare operation, 56, 81–82. *See also* search operation.
- ComposeFrame class, 750–751
- computer systems, needs definition, 213–214
- configuration
 - backing up and restoring, 543
 - changing using LDAP, 173
 - Directory Server Configuration, Command, and File Reference*, 173
 - managing, 27–28
- configuration files
 - backup and restore, 542
 - `dse.ldif`, 173
 - `notify.conf`, 605
 - schema, backup and restore, 542

- configuring
 - cascaded replication, 403
 - distributed directories, 345–348
 - Netscape Directory Server, 173–176
 - schemas, 285–286, 301
 - user preferences, 28
 - conflict resolution, 384–388
 - connecting servers, 345–348
 - connection hijacking, 412
 - connection timeouts, 622
 - consistency, 238, 375–377
 - constraints, data element values, 245–246. *See also* value constraint plug-in.
 - consumers, 246–247, 375
 - continuous mode for the `ldapmodify` command, 112
 - control operations. *See* authentication and control operations.
 - controls
 - definition, 59, 124
 - Entry Change Notification Response, 128–130
 - ManageDSAIT, 128
 - Password Expired, 137–138
 - Password Expiring, 137–138
 - Persistent Search Request, 128–130
 - Proxied Authorization, 136–137
 - Server-Side Sorting Request, 130–131
 - Server-Side Sorting Response, 130–131
 - VLV (Virtual List View) Request, 132–136
 - VLV (Virtual List View) Response, 132–136
 - convergence, 375–377
 - copying directories. *See* replication.
 - copying to/from data sources
 - migration, 763–764
 - N-way join, 768–770, 783–793
 - one-way synchronization, 764–766, 783–793
 - two-way synchronization, 766–768
 - virtual synchronization, 770–773
 - corporate databases, 762
 - correcting bad data, 573
 - CoS (class of service) feature, 179
 - cost
 - backup and restore, 514–515
 - case study, 844–845
 - data maintenance, 513–514, 559
 - design phase, 502–503
 - disaster recovery, 516–517
 - evaluating directory services software, 457, 470
 - hardware
 - apportioning to software costs, 510
 - deployment phase, 504–507
 - upgrade and replacement, 511–512
 - maintenance contracts, 518–519
 - monitoring, 512–513
 - piloting directory services, 503–504
 - political considerations, 500
 - reductions through applications, 644–647
 - software
 - apportioning to hardware cost, 510
 - deployment phase, 507–509
 - upgrades, 509–511
 - training and support, 517–519, 567–568
 - Crack password cracking package, 447
 - `createLDAPContext()` methods, 703–705
 - creating directory entries. *See* adding, directory entries.
 - credentials, forging and stealing, 412
 - criticality of service, 228
 - CSNs (change sequence numbers), 379
 - custom probing tools, 588–592
 - dampening replication, 388
 - DAS (Directory Assistance Service) protocol, 41
 - data
 - definition, 236
 - distribution, 14–16
 - element values. *See also* attribute values.
 - characteristics of, 243–247
 - definition, 236
 - format, 244
 - number of, 245
 - ownership, 245–246
 - pointers to, 236
 - restrictions, 245–246
 - size, 244–245
 - elements. *See also* attributes.
 - analyzing, 251
 - characteristics of, 243–247
 - consumers, 246–247
 - definition, 236
 - dynamic *versus* static, 248
 - example, 249–251
 - format, 244
 - inventory (example), 803
 - needs definition, 240–243
 - number of values, 245
 - ownership, 245–246
 - relationships with other elements, 249
 - restrictions, 245–246
 - shared *versus* application-specific, 248
 - value sizes, 244–245
 - integrity, 91–93
 - maintenance. *See also* maintenance phase.
 - application-maintained data, 560–562
 - authentication and security, 567
 - centrally maintained data, 563–565
 - checking data quality, 572–574
 - correcting bad data, 573
 - cost, 513–514, 559
 - data validation, 569–570
 - definition, 557
 - developer awareness, 562
 - exception handling, 559, 571
 - importance of, 558
 - new data sources, 570–571
 - performance effects, 568–569
 - responsibility for, 559
 - source of truth method, 572
 - spot checks, 573
 - training and support costs, 567–568

- update-capable clients, 566–567
 - user-maintained data, 565–570
 - user surveys, 573
 - organization, namespace design, 310
 - owners, 802
 - partitioning, 310–311
 - policy statement, creating, 239–240
 - quality, monitoring, 591
 - reference, 309–310
 - related problems, 237–238
 - replication. *See* replication.
 - sensitivity, privacy needs definition, 421
 - translation, 772–774
 - transport, 775–776
 - users, 803
 - values. *See* data, element values.
- data design
- access control, 239
 - application needs definition, 216–217
 - case studies, 801–804, 829–830, 860
 - consistency, 238
- data elements
- analyzing, 251
 - characteristics of, 243–247
 - consumers, 246–247
 - definition, 236
 - dynamic *versus* static, 248
 - example, 249–251
 - format, 244
 - needs definition, 240–243
 - number of values, 245
 - ownership, 245–246
 - relationships with other elements, 249
 - restrictions, 245–246
 - shared *versus* application-specific, 248
 - value sizes, 244–245
- data-related problems, 237–238
- data source inventory, 242–243
- versus* designing schemas, 286
- directory content, 239
- exception handling, 239
- legal considerations, 239
- multiple storage locations, 239
- overview, 236–237
- policy statement, creating, 239–240
- political considerations, 257
- redundancy, 238
- sources of data
- administrators, 254
 - applications, 254
 - batch updates, 256–257
 - databases, 253
 - end users, 254
 - files, 253–254
 - NOSs (network operating systems), 253–254
 - other directory services, 253
 - overview, 251–253
 - replication, 255
 - synchronization, 255–256
- data sources
- administrators, 254
 - applications, 254
 - batch updates, 256–257
 - copying to/from
 - migration, 763–764
 - N-way join, 768–770, 783–793
 - one-way synchronization, 764–766, 783–793
 - two-way synchronization, 766–768
 - virtual synchronization, 770–773
 - databases, 253
 - definition, 236
 - end users, 254
 - files, 253–254
 - inventory, 242–243
 - list of, 761–763
 - NOSs (network operating systems), 253–254
 - other directory services, 253
 - overview, 251–253
 - replication, 255
 - security, 776
 - synchronization, 255–256
- databases. *See also* directory partitioning.
- corporate, 762
 - as data source, 253
 - versus* directories, 29–30, 32–33
 - embedding in applications, 30
 - external, 762
 - homegrown, 762
 - links, 347
 - Netscape Directory Server
 - backing up, 164–165
 - bulk loading, 161
 - default, 160
 - dumping in DSML, 163–164
 - dumping to an LDIF file, 161–162
 - restoring, 165–167
- db2bak command, 164–165
- db2bak script, 539–540
- db2dsml command, 163
- db2ldif command, 161
- DDoS (distributed denial of service) attacks, 416
- delegating OID arcs, 292
- delete changetype LDIF statement, 97
- delete modifytype LDIF statement, 97–98
- delete operation, 56, 82
- deleted entries, restoring, 390
- deleted entry conflicts, 390
- deleting
 - attributes and values, 97–98
 - directory entries, 56, 82, 97
- denial of service (DoS) attacks, 415–416
- deployability, and security, 449–450
- deployment phase. *See also* production rollout.
- case studies
 - enterprise with an extranet, 871–874, 877
 - large multinational enterprise, 842–845, 850–852
 - Netscape Communications Corporation, 812–815, 819–821

- deployment phase *continued*
 - constraints on directory design
 - design openness, 224
 - overview, 211
 - political considerations, 225–226
 - prioritizing, 226
 - resources, 224
 - system administrators, 225
 - system designers, 224–225
 - definition, 202
 - description, 204–205
- dereferencing aliases, 72
- design center, 12
- design openness, 224
- design phase. *See also* needs definition.
 - case studies
 - data, 801–804, 829–830, 860
 - data element inventory, 803
 - data owners, 802
 - data users, 803
 - namespace, 805–808, 833–835, 863–865
 - needs definition, 799–801, 828–829, 859–860
 - privacy, 810–812, 839–841, 867–871
 - replication, 809–810, 836–839, 867
 - schemas, 804–805, 831–833, 861–863
 - security, 810–812, 839–841, 867–871
 - topology, 808–809, 836, 865–866
 - cost, 502–503
 - description, 202–204
- designers. *See* system designers.
- designing
 - data. *See* data design.
 - namespaces. *See* namespace design.
 - replication. *See* replication design.
 - schemas. *See* schema design.
 - security. *See* security design.
 - topology. *See* topology design.
- developing applications
 - access control decisions, 654–657
 - coexistence, 663–665
 - common mistakes, 669–671
 - common uses for, 649–658
 - cost reductions, 644–647
 - customizing your directory, 646–647
 - directory-agnostic SDKs, 662–663
 - directory-enabling, 648–649
 - directory interactions, 665–666
 - DSML tools and SDKs, 662
 - examples
 - directory-enabled finger service (lfingerd.pl), 737–746
 - LDAP address lookup in e-mail client (ICEMail), 746–756
 - resetting passwords (setpwd), 671–687
 - Web site with user profile storage (SimpleSite), 687–722
 - facilitating PKI deployment, 652–654
 - LDAP command line tools, 659
 - LDAP SDKs, 658–659
 - LDAP tag libraries, 660–661
 - leveraging existing code, 668–669
 - locating and sharing information, 649–650
 - location independence, 657–658
 - performance, 666–668
 - piloting, 668
 - prototyping, 668
 - reasons for, 644–649
 - roaming, 657–658
 - scalability, 666–668
 - tools for, 658–663
 - verifying authentication credentials, 650–652
- device and application probing, 578
- DIGEST-MD5 SASL authentication, 140–141
- directories
 - accessibility, and privacy, 423–424
 - accessing data. *See* functional model.
 - application-specific, 6
 - characteristics of
 - data distribution, 14–16
 - information extensibility, 14
 - interoperability, 21–22
 - joins, 22–24
 - performance, 19–21
 - read-to-write ratio, 13–14, 37, 248
 - replication, 16–19
 - standards, 21–22
 - transactions, 22–24
 - complementing other services, 35–36
 - content design. *See* data design.
 - data problems, troubleshooting, 628–630
 - data types, defining. *See* information model; schemas.
 - versus* databases, 29–30, 32–33. *See also* directories, characteristics of.
 - definition, 5–6
 - design center, 12
 - versus* DNS servers, 34–35
 - dynamic nature of, 6–8
 - evaluating the need for, 37
 - everyday, 5
 - versus* file systems, 33
 - flexibility, 8–10
 - versus* FTP servers, 34
 - general purpose, 6
 - information types, rules, and behavior. *See* schemas.
 - information units, defining. *See* information model; schemas.
 - integrating other data sources. *See* coexistence.
 - NOS (network operating system)-based, 6
 - offline, 5
 - online, 5–6
 - personalization, 11–12
 - purpose-specific, 6
 - querying, 56
 - security, 10–11
 - standards-based, 6, 37
 - updating, 56
 - uses for
 - authentication database, 35

- certificate location problem, 31
- configuration management, 27–28
- finding things, 25–26
- lightweight database applications, 29–30
- location independence, 29
- managing things, 26–29
- network-accessible storage device, 36
- organizing and accessing Web server information, 36–37
- PKI life cycle management, 31, 652
- searching *versus* browsing, 25
- security applications, 31
- synchronization, 27
- user configuration and preference management, 28
- versus* Web servers, 33–34
- directory-agnostic SDKs, 662–663
- Directory Assistance Service (DAS) protocol, 41
- directory design, constraints on
 - choosing an overall approach, 229
 - deployment
 - design openness, 224
 - overview, 211
 - political considerations, 225–226
 - prioritizing, 226
 - resources, 224
 - system administrators, 225
 - system designers, 224–225
 - hardware, 227
 - network, 227–228
 - prioritizing, 228–229
 - security, 228
 - software, 227
- directory-enabling existing applications
 - considering alternatives, 736–737
 - effects on directory service, 735
 - examples
 - directory-enabled finger service (lfingerd.pl), 737–746
 - LDAP address lookup in e-mail client (ICEMail), 746–756
 - hiding directory integration, 731–732
 - making capabilities visible, 732
 - problematic architecture, 733–734
 - protocol gateways, 732–733
 - reasons for, 726–730
 - transition phase, 735–736
- directory entries
 - adding auxiliary information. *See* auxiliary classes.
 - aliases, 68–69
 - change notification, 128–130
 - creating, 56, 82
 - definition, 60–62
 - deleting with delete operation, 56, 82
 - deleting with LDIF, 97
 - modifying content, 56, 84–86
 - modifying DN (renaming), 56, 83–84, 85
 - naming, 66
 - representing with DSML, 143–145
 - representing with LDIF, 93–96
- Directory Interface to X.500 Implemented Efficiently (DIXIE) protocol, 41
- directory life cycle. *See* deployment phase; design phase; maintenance phase.
- directory outages, 621–623
- directory partitioning
 - description, 332–335
 - examples, 361–369
 - multiple-partition example, 364–369
 - pros and cons, 351–354
 - single-partition example, 361–364
- directory partitions, discovery, 336
- directory requirements, privacy needs, 420–423
- directory schemas. *See* schemas.
- directory server access logs, monitoring, 606–607
- directory server configuration files, backup and restore, 542
- directory services
 - choosing software for. *See* evaluating directory services software.
 - components, 4–5
 - as data source, 253
 - definition, 4–5
 - embedding in applications, 30
 - versus* protocols, 50
 - putting into production. *See* production rollout.
 - testing. *See* piloting, directory services.
- Directory Services Markup Language (DSML), 143–145, 163–164
- disabling
 - Netscape Directory Server updates, 174
 - schema checking, 287, 813–814
 - write access to directory data, 173–176
- disaster recovery. *See also* backup and restore.
 - case studies, 815, 846, 874
 - cold-site recovery, 552–554
 - cost, 516–517
 - developing a plan, 550–552
 - directory-specific issues, 553–554
 - hot-site recovery, 552–554
 - risk assessment, 550–551
 - types of disasters, 549–550
 - vendor services, 549
- discovery of LDAP features and schema, 47, 125–127
- displayEntry subroutine, 743–744
- displayOneEntry() method, 711–712
- distinguished names (DNs). *See* DN (distinguished names).
- distributed data. *See* data, distribution.
- distributed denial of service (DDoS) attacks, 416
- distributed directories
 - authentication, 348–351
 - certificate-based client authentication, 350
 - configuring, 345–348
 - definition, 332–333
 - directory server software, 345–348
 - security implications, 351
- DIXIE (Directory Interface to X.500 Implemented Efficiently) protocol, 41

- DNs (distinguished names). *See also* RDNs (relative distinguished names).
 - base-64 encoding, 95–96
 - definition, 55
 - escaping special characters, 67–68
 - identifying replicated entries, 386
 - in namespace design, 308–309
 - naming entries, 66
 - non-ASCII, 95–96
 - restricted characters, 67–68
 - DNS servers *versus* directories, 34–35
 - DNS update capabilities, 35
 - documentation. *See* Internet drafts; publications; RFCs; standards.
 - documenting schemas, 299–300
 - `doEditProfile()` method, 699, 712–714
 - `doFind()` method, 701, 708–711
 - `doGet()` method, 699–700
 - `doLogin()` method, 701–702
 - `doLogout()` method, 699, 707
 - domains. *See* directory partitioning.
 - `doNewProfile()` method, 699, 712–714
 - `doPost()` method, 700–701
 - DoS (denial of service) attacks, 415–416
 - `doSaveProfile()` method, 701, 716–720
 - DSML (Directory Services Markup Language), 143–145, 163–164
 - DSML tools and SDKs, 662
 - dumping databases, 161–164
 - duplicating directories. *See* replication.
 - dynamic groups, 179
 - dynamic nature of directories, 6–8
 - dynamic roles, 179
 - dynamic *versus* static data elements, 248
 - e-mail, LDAP address lookup, 746–756
 - `email2LDAPDN()` method, 705–706
 - `emitProfileForm()` method, 714–716
 - enabling
 - applications for directory services. *See* directory-enabling applications.
 - schema checking, 287, 813–814
 - encryption
 - government restrictions, 429
 - server communications, 105–106
 - SSL (Secure Sockets Layer), 91–93, 105–107, 113–114, 412, 414, 417, 418
 - TLS (Transport Layer Security), 91–93, 412, 414, 417, 418
 - tools for, 417
 - enterprise numbers. *See* OIDs (object identifiers).
 - enterprise service providers (ESPs), 459–460
 - enterprise with an extranet (case study). *See also* examples; large multinational enterprise; Netscape Communications Corporation.
 - access control, delegation, 867–871
 - backup and restore, 874
 - deployment, 871–874, 877
 - design phase
 - data, 860
 - namespace, 863–865
 - needs definition, 859–860
 - privacy, 867–871
 - replication, 867
 - schemas, 861–863
 - security, 867–871
 - topology, 865–866
 - disaster recovery, 874
 - leveraging directory services, 876–877
 - maintenance phase, 874–876
 - monitoring, 876
 - motivation, 859
 - organizational overview, 856–859
 - piloting, 872–873
 - product choice, 871–872
 - production rollout, 873–874
 - summary of results, 877
 - troubleshooting, 876
- entries. *See* directory entries.
- Entry Change Notification Response control, 128–130
 - entry naming conflicts, 389
 - environmental analysis. *See* analyzing, environment.
 - equal sign (=)
 - equality operator within search filters, 74
 - in multivalued RDNs, 66
 - error handling for the `ldapmodify` command, 112
 - `escapedValue()` method, 706–707
 - escaping special characters
 - within DNs, 67–68
 - within search filters 78–80
 - ESPs (enterprise service providers), 459–460
 - `establishAddresses()` method, 751–752
 - evaluating directory services software
 - criteria
 - core features, 463
 - cost, 457, 470
 - example, 472–474
 - extensibility, 470–471
 - flexibility, 470–471
 - interoperability, 469
 - management features, 463–464
 - overview, 462–463
 - performance, 465–466
 - product completeness, 471
 - product future, 471
 - product support, 471–472
 - reliability, 464–465
 - scalability, 465–466
 - security, 466–467
 - standards compliance, 467–469
 - vendor services, 472
 - ESPs (enterprise service providers), 459–460
 - extranet applications, 459
 - gathering product information, 475–476
 - Internet-facing hosted applications, 459–460
 - intranet applications, 458–459

- lightweight database applications, 460, 462
- negotiating price, 476–477
- NOS applications, 458
- overview, 456–457
- piloting candidates, 476
- product categories, 457–462
- vendor input, 475–476
- virtual networks, 459
- event correlation, monitoring, 578
- examples. *See also* enterprise with an extranet; large multinational enterprise; Netscape Communications Corporation.
 - ACLs (access control lists), 434–438
 - data element design, 249–251
 - designing schemas, 269
 - directory-enabled finger service, 746–756
 - directory partitioning, 361–369
 - evaluating directory services software, 472–474
 - extending Netscape Directory Server, 180–197
 - finger service, directory-enabled, 737–746
 - flat namespace structure, 325–326
 - hierarchical namespace, 326–327
 - ICEMail, directory-enabled, 746–756
 - LDAP address lookup in e-mail client, 746–756
 - ldapsync tool, 783–793
 - lfingerd.pl gateway, 737–746
 - Netscape Directory Server value constraint plug-in, 180–197
 - one-way synchronization tool, 783–793
 - partitioning directories, 361–369
 - setpwd, a password resetting utility, 671–687
 - SimpleSite, a Web Site with User Profile Storage, 687–722
- exception handling, 239, 559, 571
- exclamation point (!), negation within search filters, 78
- export. *See* import/export.
- extended operations
 - Bulk Import Finished, 138–139
 - Bulk Import Start, 138–139
 - definition, 58, 124
- extending object classes. *See* subclassing.
- extensibility
 - definition, 58–59
 - evaluating directory services software, 470–471
 - information, 14
 - LDAP innovation, 47
- eXtensible Markup Language (XML), 143–145, 163–164
- extensible matching, 75–78
- extensibleObject object class, 272
- extension discovery, 125–127
- Extension for Transport Layer Security* (RFC 2830), 48, 92–93
- extensions (Netscape Directory Server value constraint plug-in example), 180–197
- external databases, 762
- EXTERNAL SASL authentication, 139–140
- extranets
 - case study. *See* enterprise with an extranet.
 - evaluating directory services software, 459
 - failure types, monitoring, 589
 - false alarms, monitoring, 593
 - feedback from piloting, 492–494, 496–497
 - file systems *versus* directories, 33
 - files as data source, 253–254
 - find.htm file, 695
 - finger service, directory-enabled, 737–746
 - firewalls, 417–418
 - flat namespace structure, example, 325–326
 - flat *versus* hierarchical namespace schemes, 315–317
 - flexibility
 - of directories, 8–10
 - evaluating directory services software, 470–471
 - focus groups, 494
 - following referrals. *See* chasing referrals.
 - forging credentials, 412
 - format
 - data elements, 244
 - schemas, 273–283
 - fractional replicas, 392–394
 - FTP servers *versus* directories, 34
 - functional model
 - authentication and control operations
 - bind operation, 86–87
 - unbind operation, 87
 - abandon operation, 87–88
 - interrogation operations
 - compare operation, 81–82
 - search filters, 74–81
 - search operation, 70–73
 - purpose of, 69
 - update operations
 - add operation, 82
 - delete operation, 82
 - modify operation, 84–86
 - modify DN (rename) operation, 83–85
 - GC (global catalog), Microsoft Active Directory, 352, 394
 - general purpose directories, 6
 - getIDWithRedirect() method, 708
 - get_rebind_credentials() function, 683
 - getResponseControls() method, 138
 - getSecondsToExpiration() method, 138
 - global catalog (GC), Microsoft Active Directory, 352, 394
 - glue entries, 394
 - goals and milestones, 212, 230–232
 - groups, 179
 - hackers, 411
 - hard failures, 579–580
 - hardware constraints, 227
 - hardware cost
 - apportioning to software costs, 510
 - deployment phase, 504–507
 - upgrade and replacement, 511–512
 - Hickman, Kipp, 418
 - hiding search filters, 80–81
 - hierarchical namespace, example, 326–327
 - hierarchies, attributes, 264–265

888 Index

- hijacking connections, 412
- homegrown databases, 762
- horizontal scalability, 17
- host-based SNMP agents, 587
- hot backups, 164
- hot-site recovery, 552–554
- Howes, Tim, 117
- HTTP digest authentication, 428
- hung connections, 622

- IANA (Internet Assigned Numbers Authority), 292
- ICEMail client, directory enabling, 746–756
- IDS (Integrated Directory Services) IETF working group, 49
- IDSs (intrusion detection systems), 418
- IETF (Internet Engineering Task Force), 42, 49
- immediate superior knowledge references, 336–337
- implementation, coexistence considerations, 780–783
- import/export
 - bulk import, 138–139
 - data interchange format. *See* LDIF.
 - DSML, 163–164
- incremental backups, 539
- incremental replication updates, 377–379
- indirect monitoring, 580, 591–592, 848
- information model, 60–63
- information privacy and integrity, 440–446
- inheritance, object class, 271–272
- `init()` method, 698–699
- installing Netscape Directory Server, 148–155
- instant messaging, 177, 179, 738
- Integrated Directory Services (IDS) IETF working group, 49
- interactive authentication and login applications, 356
- internationalization, 47, 118–119
- Internet Assigned Numbers Authority (IANA), 292
- Internet drafts. *See also* publications; RFCs; standards.
 - definition, 42
 - LDAP Client Update Protocol*, 142
 - [LDAP] over UDP/IP*, 142
 - LDAP...Browsing of Search Results*, 132
 - LDAPv3: All Operational Attributes*, 73
 - Named Subordinate References in [LDAP] Directories*, 128
 - Password Policy for LDAP Directories*, 136
 - Proxied Authorization Control*, 136
 - A Taxonomy of Methods for...Finding Servers*, 142
- Internet Engineering Task Force (IETF), 42, 49
- Internet-facing hosted applications, 459–460
- Internet resources. *See* online resources.
- Internet Security Scanner (ISS), 419
- Internet X.509 Public Key Infrastructure LDAPv2 Schema* (RFC 2587), 290
- interoperability, 21–22, 469
- interrogation operations
 - compare operation, 81–82
 - definition, 56
 - search filters, 74–81
 - search operation, 70–73

- interviews, 494
- intranet applications, 458–459
- intrusion detection systems (IDSs), 418
- IP Security Protocol (IPsec), 419
- ISO 639 (*Code for the Representation of Names of Languages*), 119
- ISO 3166 (*Codes for the Representation of Names of Countries*), 119
- ISS (Internet Security Scanner), 419

- Java API, 117, 658, 662
- The Java LDAP Application Program Interface*, 142, 658
- Java Naming and Directory Interface (JNDI) API, 118, 662, 693
- JNDI (Java Naming and Directory Interface) API, 118, 662, 693
- join attributes, 775
- joins, 22–24, 768–770, 783–793

- Kerberos, 418–419
- key pairs, 444
- keys, 444
- knowledge references, 336–337

- language codes, 118–119
- large multinational enterprise (case study). *See also* enterprise with an extranet; examples; Netscape Communications Corporation.
 - backup and restore, 846
 - cost analysis, 844–845
 - deployment, 842–845, 850–852
 - design phase
 - data, 829–830
 - namespace, 833–835
 - needs definition, 828–829
 - privacy, 839–841
 - replication, 836–839
 - schemas, 831–833
 - security, 839–841
 - topology, 836
 - disaster recovery, 846
 - leveraging directory services, 849–852
 - maintenance phase, 846–849
 - monitoring, 848–849
 - motivating factors, 826–828
 - organizational overview, 824–826
 - piloting, 843–844
 - product choice, 842
 - production rollout, 845
 - summary of results, 852–853
 - troubleshooting, 849
- latency, 217–218
- latency by attribute type, replication, 395
- LBER (Lightweight BER), 59
- LCUP (LDAP Client Update Protocol), 142
- LDAP
 - advantages, 50–51
 - command line tools, 659
 - definition, 49

- directory hierarchy *versus* UNIX file system
 - hierarchy, 63–66
- future directions, 141–145
- history and origins, 38–50
- models. *See* functional model; information model; naming model; security model.
- as monitoring tool, 580
- overview, 54–58
- typical protocol exchange, 56–57
- on the wire, 59
- LDAP: Programming...with Lightweight Directory Access Protocol*, 117
- LDAP Client Update Protocol* (LCUP), 142
- LDAP controls. *See* controls.
- LDAP Data Interchange Format (LDIF). *See* LDIF (LDAP Data Interchange Format).
- [LDAP] over UDP/IP, 142
- LDAP SDKs, 658–659
- LDAP tag libraries, 660–661
- LDAP URL Format* (RFC 2255), 48
- LDAP (v3) Attribute Syntax Definitions* (RFC 2252), 61–62
- `ldap_analyzer.pl` script, 607–615
- LDAPBIS (LDAPv3 Revision) IETF working group, 49
- LDAP...Browsing of Search Results*, 132
- `ldapcompare` command, 659
- `LDAPConnection.authentication()` methods, 140
- `ldap_create_persistentsearch_control()` function, 130
- `ldap_create_proxyauth_control()` function, 137
- `ldap_create_sort_control()` function, 131
- `ldap_create_sort_keylist()` function, 131
- `ldap_create_virtuallist_control()` function, 135
- `ldapdelete` command, 659
- `LDAPEntryChangeControl` class, 130
- LDAPEXT IETF working group, 49
- `ldaplookup()` method, 752–755
- `ldapmodify` command-line utility, 110–115, 659
- `ldap_parse_entrychange_control()` function, 130
- `ldap_parse_result()` function, 137
- `ldap_parse_sort_control()` function, 131
- `ldap_parse_virtuallist_control()` function, 135
- `LDAPPersistSearchControl` class, 130
- `ldap_probe.pl` script, 600–602
- `LDAPProxiedAuthControl` class, 137
- `ldap_sasl_bind()` function, 140
- `ldap_sasl_bind_s()` function, 140
- `ldapsearch` command, 659
- `ldapsearch` command-line utility
 - binding, 102–103
 - definition, 101
 - encrypting server communications, 105–106
 - filters, 102, 104–105
 - options, 106–110
 - retrieving a single entry, 102
 - retrieving specified attributes, 103–104
 - sample searches, 101–102
 - search base, 102
 - searching with SSL (Secure Sockets Layer), 105–106
- `LDAPSortControl` class, 131
- LDAP...Sorting of Search Results* (RFC 2891), 131
- `LDAPSortKey` class, 131
- `ldapsasl_clientauth_init()` function, 140
- `LDAPSSLSocketFactory` class, 140
- LDAPv3: All Operational Attributes*, 73
- LDAPv3: Technical Specification* (RFC 3377), 48
- LDAPv3* (RFC 2251), 47
- LDAPv3 Attribute Syntax Definitions* (RFC 2252), 47, 61–62, 274
- [LDAPv3] *Extension for Transport Layer Security* (RFC 2830), 142
- LDAPv3 extensions, 125–127. *See also* controls; extended operations; SASL authentication.
- LDAPv3 Revision (LDAPBIS) IETF working group, 49
- LDAPv3 schema format, 273–279
- LDAPv3 UTF-8 String Representation of Distinguished Names* (RFC 2253), 47
- `LDAPVirtualListControl` class, 135–136
- `LDAPVirtualListResponse` class, 136
- LDIF backup, 540–542
- LDIF (LDAP Data Interchange Format)
 - adding entries, 96–97
 - backup and restore, 540–542
 - definition, 93
 - deleting attribute values, 97–98
 - deleting attributes, 98
 - deleting entries, 97
 - dumping databases to, 161–162
 - file types, 93
 - folding long lines, 94–95
 - modifying attribute values, 97–99
 - modifying entries, 97–99
 - moving entries, 99–100
 - renaming entries, 99–100
 - representing directory entries, 93–96
 - update statements, 96–100
- `ldif2db` command, 161
- left angle, equal sign (\leq), greater than or equal to, within search filters, 75
- legal considerations, 239, 426–427
- level of service, 218
- leveraging directory services, case studies, 818–821, 849–852, 876–877
- `lfingerd.pl` gateway example, 737–746
- LFMs (log file monitors), 420
- life cycle
 - directory. *See* deployment phase; design phase; maintenance phase.
 - PKI life cycle management, 31, 652
- Lightweight BER (LBER), 59
- lightweight database applications, 29–30, 460, 462
- Lightweight Directory Access Protocol. *See* LDAP.
- locality, effects of replication, 17
- location independence, 29, 657–658
- log file monitors (LFMs), 420
- `login.htm` file, 694

890 Index

- logs
 - analyzing, 410, 580–581, 590–591
 - changelog, 379
 - directory server access, 606–607
 - LFMs (log file monitors), 420
 - operating system, 607
 - transaction, 539
- main() function, 675–680
- maintenance phase. *See also* data, maintenance.
 - case studies, 815–818, 846–849, 874–876
 - cost of contracts, 518–519
 - definition, 202
 - description, 206–207
 - schemas, 300
- man-in-the-middle attacks, 414
- ManagedSAsIT control, 128
- management features, evaluating directory services
 - software, 463–464
- Management Information Base (MIB), 584–587
- mandatory attributes, 268
- manuals. *See* Internet drafts; publications; RFCs; standards.
- mapping
 - networks, 214–215
 - organizational structure and geography, 213
- marketing and publicity plan, 528–529
- masquerading, 415
- matching rules, 61, 265, 267
- message-oriented protocols, 54
- messaging applications, 356–357
- MIB (Management Information Base), 584–587
- Microsoft Active Directory, 345, 394
- migration, 763–764
- milestones and goals, 212, 230–232
- mix-in (auxiliary) object classes, 268, 295
- moddn changetype LDIF statement, 99–100
- modify changetype LDIF statement, 97–99
- modify DN (rename) operation, 56, 83–84, 85
- modify operation, 56, 84–86. *See also* ldapmodify
 - command-line utility.
- modifying
 - attribute values with LDIF, 97–99
 - directory entries, 56, 84–86
 - DNs (distinguished names), 56, 83–84, 85
 - entries with LDIF, 97–99
 - entry names, 56, 83–84, 85
- modifytype LDIF statement, 97
- monitoring. *See also* troubleshooting.
 - case studies, 817–818, 848–849, 876
 - coexistence, 782–783
 - conceptual models, 578–579
 - cost, 512–513
 - data quality, 591
 - device and application probing, 578
 - directory server access logs, 606–607
 - event correlation, 578
 - failure types, 589
 - false alarms, 593
 - hard failures, 579–580
 - indirect, 580, 591–592
 - introduction, 578–582
 - LDAP traffic, 59
 - log file analysis, 580–581, 590–591
 - messages, 584
 - methods, 580–581
 - MIB (Management Information Base), 584
 - minimizing failure effects, 596–597
 - notification, 578, 592–596
 - operating system logs, 607
 - operating system performance data, 580
 - performance analysis, 578, 605–616
 - principles, 581–582
 - problem correction, 598
 - problem histories, 581
 - problem reports, 598–599
 - problem spotting, 616
 - raw usage data, 606–607
 - reported problems, 638
 - root causes, 597–598
 - sample utility, 599–605
 - synchronization processes, 591
 - taking action, 596–599
 - tools for
 - custom probing tools, 588–592
 - host-based SNMP agents, 587
 - LDAP (Lightweight Directory Access Protocol), 580
 - MIB (Management Information Base), 585–587
 - NMSs (network management systems), 583–587
 - SNMP (Simple Network Management Protocol), 580, 583–587
 - traps, 584
 - trend spotting, 616
 - unobtrusiveness, 581
- moving entries, 99–100
- Mozilla project, 115–116, 658, 737, 817
- multimaster replication, 383–391, 544
- multiple storage locations, 239
- multivalued RDNs, namespace design, 308, 320
- mutual authentication, 417
- N-way join, 768–770, 783–793
- N+1 directory problem, 27
- name resolution
 - chaining, 343–344
 - client-side processing, 339–343, 344–345
 - definition, 337
 - LDAP referrals, 339–341
 - purported names, 338–339
 - search result continuation references, 339–343
 - server-side processing, 343–345
- Named Subordinate References in [LDAP] Directories*, 128
- namespace design
 - access control, 311
 - application support, 312
 - case studies, 805–808, 833–835, 863–865
 - data organization, 310
 - data reference, 309–310

- flat structure, example, 325–326
- hierarchical, example, 326–327
- motivating factors, 324
- multivalued RDNs, 308, 320
- needs definition
 - application considerations, 320–321
 - flat *versus* hierarchical schemes, 315–317
 - future needs, 324
 - naming attributes, 318–320, 322–323
 - naming RDNs, 322–323
 - privacy considerations, 323–324
 - suffixes, 313–315
- overview, 305–306
- partitioning data, 310–311
- purposes of a namespace, 309–313
- RDNs, 308, 320
- replication, 311
- reuse policy, 322
- structure of a namespace, 306–309
- topology design, 359–360
- naming
 - directory entries, 66
 - RDNs, 322–323
 - schema attributes, 262, 291
- naming attributes, 318–320, 322–323
- naming context. *See* directory partitioning.
- naming model, 63–69
- needs definition, case studies, 799–801, 828–829, 859–860
- Net::LDAP Perl-LDAP modules, 659
- Netscape 7.0, 177
- Netscape Certificate Management System, 177
- Netscape Communications Corporation (case study).
 - See also* enterprise with an extranet; examples;
 - large multinational enterprise.
 - backup and restore, 815
 - deployment phase, 812–815, 819–821
 - design phase
 - data, 801–804
 - data element inventory, 803
 - data owners, 802
 - data users, 803
 - namespace, 805–808
 - needs definition, 799–801
 - privacy, 810–812
 - replication, 809–810
 - schemas, 804–805
 - security, 810–812
 - topology, 808–809
 - disaster recovery, 815
 - leveraging directory services, 818–821
 - maintenance phase, 815–818
 - monitoring, 817–818
 - motivating factors, 799
 - organizational overview, 798–799
 - piloting, 813
 - product choice, 813
 - production rollout, 814–815
 - schema checking, enabling, 813–814
 - summary of results, 821–822
- Netscape Communicator, 177
- Netscape Delegated Administrator, 177–178
- Netscape Directory Server
 - access control, 167–173
 - databases
 - backing up, 164–165, 538–543
 - bulk loading, 161
 - default, 160
 - dumping to a DSML file, 163–164
 - dumping to an LDIF file, 161–162
 - restoring, 165–167
 - default port, 151
 - disabling updates, 174
 - distribution and chaining, 346–348
 - extending (value constraint plug-in example), 180–197
 - features, 178–180
 - history, 176–177
 - installing, 148–155
 - LDAP-enabled companion products, 177–178
 - loading sample data, 152–155
 - product focus, 177–178
 - Proxied Authorization, 167–173
 - proxy right, 167–173
 - reconfiguring with LDAP, 173–176
 - searching, 155–160
 - system requirements, 148
- Netscape Directory Server Administrator's Guide*, 91, 105
- Netscape LDAP C SDK, 658
- Netscape LDAP Java SDK, 658
- network intrusion detection systems (NIDSs), 419
- network management systems (NMSs), 583–587
- network operating system (NOS)-based directories, 6
- network operating systems (NOSs), 253–254, 761
- networks
 - constraints on system design, 227–228
 - managing, 583–587
 - mapping, 214–215
 - monitoring, 419, 583–587
 - needs definition, 214–215
 - security and privacy needs definition, 424–425
 - security tools, 419
 - sniffing, 412
 - topology design, 358–359
 - virtual, 459
- NIDSs (network intrusion detection systems), 419
- NMSs (network management systems), 583–587
- non-ASCII attribute values, 95–96
- non-ASCII DNs, 95–96
- NOS applications, 458
- NOS (network operating system)-based directories, 6
- NOSs (network operating systems), 253–254, 761
- notification of problems, 578, 592–596, 633–635
- `notify.conf` configuration file, 605
- `notify.pl` script, 602–604
- Novell eDirectory, 345

- OASIS (Organization for the Advancement of Structured Information Standards), 143
- object classes, designing schemas
 - abstract, 268
 - allowed (optional) attributes, 268, 274–277
 - ASN.1 format, 282–283
 - auxiliary (mix-in), 268, 279, 295–297
 - example, 269
 - extensibleObject, 272
 - inheritance, 271–272
 - kind of object, 268
 - LDAPv3 format, 277–279
 - mandatory attributes, 268
 - mix-in (auxiliary), 268, 295
 - multiple, 269–270
 - names, 268
 - overview, 267–269
 - structural, 268, 278
 - subclassing, 271–272, 293–295
 - superclasses, 271–272
 - superior classes, 271–272
- object identifiers (OIDs), 76–77, 124
- objectClasses attribute, 274–277
- offline directories, 5
- OIDs (object identifiers), 76–77, 124, 292
- one-way authentication, 417
- one-way synchronization, 764–766, 783–793
- online comments, user feedback, 494
- online directories, 5–6
- online backup and restore, 539
- online resources
 - ADSI API, 118
 - APIs, 115–116, 117–118
 - C language SDK, 115–116
 - Crack password cracking package, 447
 - IETF (Internet Engineering Task Force), 42
 - IETF working groups, 49
 - Java API, 117
 - JNDI API, 118
 - LDAPBIS IETF Working Group, 141
 - LDAPv3: *All Operational Attributes Internet Draft*, 73
 - Mozilla project, 115–116
 - obtaining OIDs, 292
 - OpenLDAP Project, 115–116
 - password cracking, 447
 - Perl API, 117
 - Python API, 117
 - SDKs, 115–116
 - security tools, 419, 420
 - Snort network intrusion detection system, 419
 - Sun Microsystems, 115
 - Swatch log file monitor package, 420
 - Tripwire system integrity verifier package, 420
- OpenLDAP Project, 115–116
- operating system logs, 607
- operating system performance data, 580
- operational attributes, 62, 263
- operations, canceling, 56
- OR operators within search filters, 78
- organization data. *See* naming model.
- Organization for the Advancement of Structured Information Standards (OASIS), 143
- organizational structure and geography, needs
 - definition, 213
- originating writes, 387
- OSI-DS IETF working group, 49
- ownership of data, 245–246
- parentheses (()), grouping terms within search filters, 78
- partition root, 333
- partitioning. *See* data, partitioning; directory partitioning.
- Password Expired control, 137–138
- Password Expiring control, 137–138
- Password Policy for LDAP Directories*, 136
- passwords
 - cracking, 447
 - encrypting, 428–430
 - expiration, 137–138
 - hashing, 89
 - policies, 446–448
 - resetting, sample utility, 671–687
 - rules for choosing, 447
 - simple, 428
 - zero-length, 670
- performance
 - application needs definition, 217–218
 - applications for, 666–668
 - coexistence considerations, 781
 - data maintenance effects, 568–569
 - directory characteristic, 19–21
 - effects of replication, 17
 - evaluating directory services software, 465–466
 - monitoring, 578, 605–616
 - problems, troubleshooting, 623–627
 - replication design, 400–402
 - testing, 466
 - vendor-supplied figures, 401
- Perl API, 117
- PerLDAP Perl module, 659, 737, 787, 817
- Persistent Search Request control, 128–130
- personalizing directories, 11–12
- physical access, 413
- physical security, privacy needs definition, 424–425
- piloting
 - case studies, 813, 843–844, 872–873
 - directory services. *See also* production rollout.
 - applying the results, 496–497
 - collecting feedback, 492–494, 496–497
 - cost, 503–504
 - documentation, 485–487
 - goals, 484
 - prepilot testing, 482–483
 - prospective software purchases, 476
 - rollout, 491–492
 - scaling up, 495–496
 - scope, 484–485
 - setting up the environment, 489–491

- timeline, 484–485
 - training materials, 485–487
 - user categories, 486–487
 - users, selecting, 487–489
- new applications, 668
- PKI
 - certificate life cycle management, 31, 652
 - facilitating deployment, 652–654
 - overview, 444–445
 - privacy and security, 443–446
 - revocation, 445
- plus sign (+), in search operations, 73
- pointers to data element values, 236
- political considerations
 - cost, 500
 - data design, 257
 - deployment constraints, 225–226
 - topology design, 361
- pound sign (#), comment indicator, 605, 783
- prefix notation for search filters, 78
- presence filters, 75
- `print_ldap_error()` function, 683
- prioritizing
 - application needs definition, 219–220
 - constraints, 228–229
 - deployment constraints, 226
 - user needs and expectations, 223
- privacy
 - application needs definition, 219
 - case studies, 810–812, 839–841, 867–871
 - coexistence considerations, 774–776
 - information, 440–446
 - namespace design, 323–324
 - needs definition
 - administration, 422–423
 - applicable laws, 426–427
 - corporate policies, 426–427
 - data sensitivity, 421
 - directory accessibility, 423–424
 - directory requirements, 420–423
 - environment analysis, 423–425
 - network environment, 424–425
 - physical security, 424–425
 - read/write access, 420
 - replication, 421–422
 - synchronization, 421–422
 - user community, 423
 - user expectations, 425–426
 - TLS (Transport Layer Security), 91–93, 412, 414, 417, 418
 - user information, 448–449
 - user needs and expectations, 222
- problem reports, 598–599, 638–639
- problems. *See* monitoring; troubleshooting.
- product choice, case studies, 813, 842, 871–872
- product completeness, software criteria, 471
- product evaluation. *See* evaluating directory services software.
 - product future, software criteria, 471
 - product support, software criteria, 471–472
 - production rollout. *See also* piloting, directory services.
 - case studies, 814–815, 845, 873–874
 - incremental approach, 530
 - maintaining focus, 530
 - potential problems, 532
 - prerequisite tasks, 525–526
 - publicity and marketing plan, 528–529
 - required resources, 525
 - rollout plan, 527
 - success criteria, 527–528
 - thinking ahead, 530–533
 - timing, 529–530
 - protocol operations, 56–58
 - prototyping new applications, 668
 - Proxied Authorization, 136–137, 167–173
 - Proxied Authorization Control*, 136
 - proxy right, 136, 167–173
 - publications. *See also* Internet drafts; RFCs.
 - Directory Server Configuration, Command, and File Reference*, 173
 - LDAP: Programming...with Lightweight Directory Access Protocol*, 117
 - Netscape Directory Server 6 Administrator's Guide*, 91, 105
 - Netscape Directory Server 6 Installation Guide*, 148
 - publicity and marketing plan, 528–529
 - purported names, 338–339
 - purpose-specific directories, 6
 - Python-LDAP module, 117, 659
- querying directories, 56
- Quipu, 40
- `randompwd()` function, 684–685
- `randomword()` function, 685–686
- RDNs (relative distinguished names). *See also* DNs (distinguished names).
 - definition, 66
 - multivalued, 66–67, 308
 - in namespace design, 308, 320
- read-to-write ratio, 13–14, 37, 248
- read/write access, privacy needs definition, 420
- redundancy, data design, 238
- reference material. *See* Internet drafts; publications; RFCs; standards.
- referrals
 - chasing, 342, 381, 670
 - definition, 339–341
 - direct manipulation, 128
 - LDAP innovation, 47
 - rebind function, 670, 679, 683
- referring to data. *See* naming model.
- refused connections, 622
- rejects file, 112
- relative distinguished names (RDNs). *See* RDNs (relative distinguished names).

894 Index

- reliability
 - versus* availability, 18
 - effects of replication, 17
 - evaluating directory services software, 464–465
 - replication design, 398–400
- rename (modify DN) operation, 56, 83–84, 85
- renaming
 - directory entries (changing DN), 56, 83–84, 85
 - LDIF, 99–100
 - modify DN (rename) operation, 56, 83–84, 85
- replace modifytype LDIF statement, 97–98
- replica update vectors (RUVs), 387–388
- replicas
 - maximum number of, 402–404
 - refreshes, 377–379
 - replication updates *versus* client updates, 387
- replication
 - access control, 396
 - ACLs (access control lists), 396
 - agreements, 375
 - as backup and restore tool, 543–545
 - case studies, 809–810, 836–839, 867
 - changelog, 379
 - client updates *versus* replica updates, 387
 - clock synchronization, 385–386
 - conflict resolution, 384–388
 - consistency, 375–377
 - consumers, 375
 - convergence, 375–377
 - CSNs (change sequence numbers), 379
 - dampening, 388
 - of data sources, 255
 - definition, 16
 - deleted entries, restoring, 390
 - deleted entry conflicts, 390
 - directory characteristic, 16–19
 - entry naming conflicts, 389
 - fractional replicas, 392–394
 - GC (global catalog), 352, 394
 - glue entries, 394
 - granularity, 386
 - horizontal scalability, 17
 - incremental updates, 377–379
 - initial population, 379–380
 - latency by attribute type, 395
 - multimaster strategy, 383–391
 - namespace design, 311
 - originating writes, 387
 - privacy needs definition, 421–422
 - protocols, 391
 - purpose of, 272
 - reasons for, 16–17
 - replica refreshes, 377–379
 - RUVs (replica update vectors), 387–388
 - scheduling, 395
 - schemas, 395–396
 - sequence numbers, 385–386
 - server-to-server, 179
 - single-master strategy, 381–383
 - single-value constraint conflicts, 391
 - sparse replicas, 392–394
 - subsets of directory information, 392–394
 - suppliers, 375
 - synthetic time, 385
 - tombstone entries, 390
 - total updates, 377–379
 - unique identifiers, 386
 - unit of replication, 375
 - update conflict resolution policy, 383–384
 - update resolution policies, 389–391
 - wall-clock time, 385
- replication design
 - capacity planning, 401
 - cascaded configuration, 403
 - choosing a solution, 404
 - maximum number of replicas, 402–404
 - overhead considerations, 404
 - overview, 396–398
 - performance, 400–402
 - reliability, 398–400
 - synchronization traffic reduction, 403
 - vendor-supplied performance figures, 401
- reportError() method, 721–722
- repositories of data. *See* data sources.
- Requests for Comments. *See* RFCs.
- resetpwd() function, 680–681
- resources, deployment constraints, 224
- restore. *See* backup and restore; disaster recovery.
- restricted characters
 - DNs (distinguished names), 67–68
 - search filters, 78–79, 80
- restrictions. *See* constraints.
- reuse policy, namespace design, 322
- RFCs. *See also* Internet drafts; publications; standards.
 - 2222 (SASL...), 139
 - 2251 (LDAP (v3)), 47
 - 2252 (LDAP (v3) Attribute Syntax Definitions), 47, 61–62, 274
 - 2253 (LDAP (v3) UTF-8 String Representation of Distinguished Names), 47
 - 2254 (String Representation of LDAP Search Filters), 47
 - 2255 (LDAP URL Format), 48
 - 2256 (Summary of the X.500(96) User Schema for Use with LDAPv3), 48
 - 2587 (Internet X.509 Public Key Infrastructure LDAPv2 Schema), 290
 - 2820 (Access Control Requirements for LDAP), 142
 - 2829 (Authentication Methods for LDAP), 48, 90, 125
 - 2830 ([LDAPv3] Extension for Transport Layer Security), 48, 92–93, 142
 - 2831 (Using Digest Authentication as a SASL Mechanism), 140
 - 2891 (LDAP...Sorting of Search Results), 131
 - 3377 (LDAP (v3): Technical Specification), 48
- right angle, equal sign (=), greater than or equal to operator within search filters, 75
- risk assessment, disaster recovery, 550–551

- roaming, 657–658
- roles, 179
- rollback, definition, 23
- rollout. *See* production rollout.
- root DSE, 47, 125–127, 336
- Ruby/LDAP module, 659
- RUVs (replica update vectors), 387–388

- SASL... (RFC 2222), 139
- SASL authentication
 - definition, 124–125
 - description, 431
 - DIGEST-MD5, 140–141
 - EXTERNAL, 139–140
- SASL bind operation, 86–87
- SASL (Simple Authentication and Security Layer), 59, 419
- SATAN (Security Administrator Tool for Analyzing Networks), 419
- scalability. *See also* replication.
 - evaluating directory services software, 465–466
 - horizontal, 17
- scheduling replication, 395
- schema design
 - ASN.1 format, 280–283
 - attributes, 274–277
 - allowed (optional), 268, 274–277
 - hierarchies, 264–265
 - matching rules, 265, 267
 - naming, 262, 291
 - operational, 263
 - subtypes, 264–265
 - supertypes, 264–265
 - syntax, 265, 266
 - type example, 263–264
 - usage indicators, 262, 276
 - values, 262
 - changing existing schemas, 301
 - configuration, 285–286, 301
 - versus* designing data, 286
 - documenting schemas, 299–300
 - elements
 - defining, 291–299
 - modifying, 293
 - summary of, 272–273
 - evolution, 300
 - formats, 273–283
 - LDAPv3 format, 273–279
 - maintenance, 300
 - new object types, 297–298
 - object classes
 - abstract, 268
 - allowed (optional) attributes, 268, 274–277
 - ASN.1, 282–283
 - auxiliary (mix-in), 268, 279, 295–297
 - example, 269
 - extensibleObject, 272
 - inheritance, 271–272
 - kind of object, 268
 - LDAPv3, 277–279
 - mandatory attributes, 268
 - mix-in (auxiliary), 268, 279, 295–297
 - multiple objects, 269–270
 - names, 268
 - overview, 267–269
 - structural, 268, 278
 - subclassing, 271–272, 293–295
 - superclasses, 271–272
 - superior classes, 271–272
 - OIDs, obtaining and assigning, 292
 - overview, 285–287
 - predefined, sources of, 287–290
 - purpose of schemas, 260–261
 - review boards, 300
 - schema checking, description, 283–284
 - schema checking, disabling, 287
 - subschema entries, 274
 - tips for, 298–299
 - upgrading directory service software, 301
 - using existing schemas, 285
- schemas
 - adding to directory servers, 289–290
 - ASN.1 format, 280–283
 - case studies, 804–805, 831–833, 861–863
 - changing, 301
 - checking, description, 283–284
 - checking, disabling, 287
 - checking, enabling, 813–814
 - configuration, 285–286, 301
 - configuration files, backup and restore, 542
 - definition, 14, 62–63, 259–260
 - versus* designing data, 286
 - directory-enabled applications, 287–288
 - from directory vendors, 289
 - discovery, 47
 - documenting schemas, 299–300
 - evolution, 300
 - formats, 273–283
 - LDAPv3 format, 273–279
 - maintenance, 300
 - new object types, 297–298
 - OIDs, obtaining and assigning, 292
 - predefined, sources of, 287–290
 - purpose of, 260–261
 - replication, 395–396
 - reusing existing, 285
 - review boards, 300
 - standard, 288–289
 - subschema entries, 274
- script kiddies, 411
- SDKs, 115–116
- search base, 70, 102
- search filters
 - () (parentheses), grouping search terms, 78
 - & (ampersand), AND operator, 78
 - * (asterisk), wildcard, 74
 - = (equal sign), equality operator, 74
 - ! (exclamation point), negation operator, 78

896 Index

- search filters *continued*
 - <= (left angle, equal sign), greater than or equal to operator, 75
 - >= (right angle, equal sign), greater than or equal to operator, 75
 - | (vertical bar), OR operator, 78
 - ~= (tilde, equal sign), approximation operator, 74–75
 - combining terms, 78
 - escaping special characters, 78–79, 80
 - extensible matching, 75–78
 - hiding from users, 80–81
 - ldapsearch utility, 102, 104–105
 - list of, 79
 - OIDs (object identifiers), 76–77
 - AND operator, 78
 - OR operator, 78
 - prefix notation, 78
 - presence, 75
 - restricted characters, 78–79, 80
 - specifying, 72
 - substrings, 74
- search operation. *See also* compare operation.
 - abusive searches, 669
 - alias dereferencing, 72
 - all entries below an entry, 80
 - all entries within a subtree, 80
 - definition, 56
 - filters, 72
 - Netscape Directory Server, examples, 155–160
 - parameters, 70–73
 - requests, canceling, 56, 87–88
 - retrieving a single entry, 102
 - retrieving all operational attributes, 73
 - retrieving attributes only, 72–73
 - retrieving specified attributes, 103–104
 - sample searches, 101–102
 - single entries, 80
 - size limit, 72
 - with SSL (Secure Sockets Layer), 105–106
 - starting point, specifying, 70
 - time limit, 72
 - types of searches, 80
- search results
 - continuation references, 339–343
 - sorting, 130–131
 - viewing, 132–136
- search scope, 70–71, 102
- searching *versus* browsing, 25
- Secure Shell (SSH), 419
- Secure Sockets Layer (SSL), 91–93, 105–107, 113–114, 180, 412, 414, 417, 418
- security. *See also* authentication; passwords.
 - application needs definition, 219
 - backdoor access, 413
 - case studies, 810–812, 839–841, 867–871
 - certificate authority, 444
 - certificate issuance, 444
 - certificate revocation list, 445
 - certificates, 444
 - coexistence considerations, 774–776
 - connection hijacking, 412
 - constraints on system design, 228
 - credential forging, 412
 - credential stealing, 412
 - data maintenance, 567
 - DDoS (distributed denial of service) attacks, 416
 - delegation risks, 869
 - directory characteristic, 10–11
 - distributed directory implications, 351
 - DoS (denial of service) attacks, 415–416
 - encryption
 - government restrictions, 429
 - server communications, 105–106
 - SSL (Secure Sockets Layer), 91–93, 105–107, 113–114, 412, 414, 417, 418
 - TLS (Transport Layer Security), 91–93, 412, 414, 417, 418
 - tools for, 417
 - evaluating directory services software, 466–467
 - guidelines, 408–409
 - hackers, 411
 - key pairs, 444
 - keys, 444
 - LDAP as server administration protocol, 175
 - LDAP innovations, 47
 - log analysis, 410
 - man-in-the-middle attacks, 414
 - masquerading, 415
 - network sniffing, 412
 - physical, privacy needs definition, 424–425
 - physical access, 413
 - PKI revocation, 445
 - problems, troubleshooting, 630–632
 - purpose of, 409–411
 - script kiddies, 411
 - software bugs, 413–414
 - threats, 411–416
 - trawling, 410
 - Trojan horses, 413–414
 - unauthorized access, 412–414
 - unauthorized tampering, 414–415
- Security Administrator Tool for Analyzing Networks (SATAN), 419
- security applications, 31
- security design
 - access control, 432–434
 - access control policy, 433–434
 - ACLs (access control lists)
 - description, 432–433
 - examples, 434–438
 - placement, 439–440
 - administrative controls, 446–448
 - anonymous authentication, 427–428
 - authentication, 427–431
 - certificate authentication, 430–431
 - deployability, 449–450
 - HTTP digest authentication, 428

- information privacy and integrity, 440–446
- password policies, 446–448
- passwords, encrypting, 428–430
- passwords, simple, 428
- PKI, 443–446
- SASL authentication, 431
- user privacy, 448–449
- security model
 - access control, 90–91
 - authentication, 88, 90
 - binding, 89
 - TLS (Transport Layer Security), 91–93, 412, 414, 417, 418
- security needs definition
 - administration, 422–423
 - applicable laws, 426–427
 - corporate policies, 426–427
 - data sensitivity, 421
 - directory accessibility, 423–424
 - directory requirements, 420–423
 - environment analysis, 423–425
 - network environment, 424–425
 - physical security, 424–425
 - read/write access, 420
 - replication, 421–422
 - synchronization, 421–422
 - user community, 423
 - user expectations, 425–426
- security tools
 - auditing, 417
 - authentication, 417, 418
 - Crack password cracking package, 447
 - encryption, 417
 - firewalls, 417–418
 - IDSs (intrusion detection systems), 418
 - IPsec (IP Security Protocol), 419
 - ISS (Internet Security Scanner), 419
 - Kerberos, 418–419
 - LFMs (log file monitors), 420
 - mutual authentication, 417
 - NIDSs (network intrusion detection systems), 419
 - one-way authentication, 417
 - online resources, 419, 420
 - SASL (Simple Authentication and Security Layer), 419
 - SATAN (Security Administrator Tool for Analyzing Networks), 419
 - signing, 417
 - SIVs (system integrity verifiers), 419–420
 - Snort network intrusion detection system, 419
 - SSH (Secure Shell), 419
 - SSL (Secure Sockets Layer), 91–93, 105–107, 113–114, 412, 414, 417, 418
 - Swatch log file monitor package, 420
 - TLS (Transport Security Layer), 91–92, 412, 414, 417, 418
 - Tripwire system integrity verifier package, 420
 - two-way authentication, 417
- sequence numbers, replication, 385–386
- Server-Side Sorting Request control, 130–131
- Server-Side Sorting Response control, 130–131
- server software, 100
- sessions, terminating, 56
- setpwd utility example, 671–687
- setpwd.c prelude, 672–674
- setting goals and milestones, 230–232
- signing, 417
- simple authentication, 88
- Simple Authentication and Security Layer (SASL), 59, 419
- Simple Network Management Protocol (SNMP), 580, 583–587
- SimpleSite example, a Web Site with User Profile Storage, 687–722
- SimpleSiteServlet.java, 695–698
- single-master replication, 381–383, 546–547
- single-value constraint conflicts, 391
- SIVs (system integrity verifiers), 419–420
- size, data element values, 244–245
- slapd (standalone LDAP daemon), 45–46
- Smith, Mark, 117
- snapshot restores, 540
- sniffers, monitoring LDAP traffic, 59
- SNMP (Simple Network Management Protocol), 580, 583–587
- Snort network intrusion detection system, 419
- software
 - bugs, security risks, 413–414
 - constraints on system design, 227
 - cost
 - apportioning to hardware cost, 510
 - deployment phase, 507–509
 - upgrades, 509–511
 - directory service, choosing. *See* evaluating directory services software.
- sorting search results, 130–131
- source of truth method, 572
- sources of data. *See* data sources.
- sparse replicas, 392–394
- spot checks for bad data, 573
- SSH (Secure Shell), 419
- SSL (Secure Sockets Layer), 105–106, 180, 418
- standalone directory service, 45–46
- standalone LDAP daemon (slapd), 45–46
- standard directories, 38–41
- standards. *See also* Internet drafts; RFCs.
 - directory characteristic, 21–22
 - DNS update capabilities, 35
 - ISO 639 (*Code for the Representation of Names of Languages*), 119
 - ISO 3166 (*Codes for the Representation of Names of Countries*), 119
 - in the works, 141–142
- standards-based directories, 6, 37
- standards compliance, software evaluation criteria, 467–469
- standards documents. *See* Internet drafts; RFCs, standards.

- standards groups
 - ASID (Access, Searching, and Indexing of Directories) IETF working group, 49
 - IDS (Integrated Directory Services) IETF working group, 49
 - IETF (Internet Engineering Task Force), 42, 49
 - LDAPBIS (LDAPv3 Revision) IETF working group, 49
 - LDAPEXT (LDAP Extensions) IETF working group, 49
 - OASIS (Organization for the Advancement of Structured Information Standards), 143
 - OSI-DS IETF working group, 49
- stealing credentials, 412
- String Representation of LDAP Search Filters* (RFC 2254), 47
- structural object classes, 268, 278
- subarcs, OID, 77
- subclassing object classes, 271–272, 293–295
- subordinate knowledge references, 336–337
- subschema entries, 274
- substring search filters, 74
- subtypes, 264–265
- suffixes, namespace design, 313–315
- Summary of the X.500(96) User Schema for Use with LDAPv3* (RFC 2256), 48
- Sun Microsystems, 115
- superclasses, 271–272
- superior classes, 271–272
- supertypes, 264–265
- suppliers, replication, 375
- support costs, 517–519, 567–568
- Swatch log file monitor package, 420
- synchronization
 - of data sources, 255–256
 - monitoring, 591
 - privacy needs definition, 421–422
 - role of directories, 27
 - traffic, reducing, 403
 - syntax associated with attribute types, 61–62, 265–266
- synthetic time, 385
- system administration
 - privacy needs definition, 422–423
 - security controls, 446–448
- system administrators
 - as data source, 254
 - as deployment constraints, 225
- system designers, as deployment constraints, 224–225
- system integrity verifiers (SIVs), 419–420
- A Taxonomy of Methods for...Finding Servers*, 142
- testing directory services. *See* piloting, directory services.
- throughput
 - tilde, equal sign (~=) approximation operator within search filters, 74–75
- TLS (Transport Layer Security), 91–93, 412, 414, 417, 418
- tombstone entries, 390
- tools for
 - auditing, 417
 - authentication, 417, 418
 - coexistence, 781–782
 - custom probing, 588–592
 - developing applications, 658–663
 - encryption, 417
 - monitoring, 580, 583–592
 - security, 417–420
- topology case studies, 808–809, 836, 865–866
- topology design
 - connecting servers, 345–348
 - distributed directories. *See also* name resolution.
 - authentication, 348–351
 - certificate-based client authentication, 350
 - configuring, 345–348
 - definition, 332–333
 - directory server software, 345–348
 - security implications, 351
 - factors affecting
 - address book applications, 356
 - authentication applications, 356
 - directory-enabled applications, 354–357
 - directory namespace design, 359–360
 - directory server software capabilities, 357–358
 - interactive authentication and login applications, 356
 - messaging applications, 356–357
 - physical network topology, 358–359
 - political considerations, 361
 - knowledge references, 336–337
 - name resolution
 - chaining, 343–344
 - client-side processing, 339–343, 344–345
 - definition, 337
 - LDAP referrals, 339–341
 - purported names, 338–339
 - search result continuation references, 339–343
 - server-side processing, 343–345
 - overview, 332–335
 - partition discovery, 336
 - partition relationships. *See* knowledge references; name resolution.
 - partitioning directories
 - description, 332–335
 - examples, 361–369
 - multiple-partition example, 364–369
 - pros and cons, 351–354
 - single-partition example, 361–364
- total replication updates, 377–379
- training costs, 517–518, 567–568
- transaction logs, 539
- transactions, 22–24
- Transport Layer Security (TLS), 91–93, 412, 414, 417, 418
- traps (monitoring messages), 584
- trawling, 410
- trends, spotting, 616

- Tripwire system integrity verifier package, 420
- Trojan horses, 413–414
- troubleshooting. *See also* monitoring.
 - assessing the problem, 633–635
 - case studies, 849, 876
 - change control policy, 638
 - coexistence, 782
 - connection timeouts, 622
 - containing damage, 635
 - directory data problems, 628–630
 - directory outages, 621–623
 - discovering problems, 620–621
 - hung connections, 622
 - long-term fixes, 636–637
 - monitoring the problem, 638
 - notifying affected persons, 633–635
 - performance problems, 623–627
 - preventing recurrences, 637–638
 - problem reports, 638–639
 - refused connections, 622
 - security problems, 630–632
 - short-term fixes, 635–636
 - step-by-step process, 632–639
- tuning coexistence, 782
- two-way authentication, 417
- two-way synchronization, 766–768
- UCS Transformation Format 8 (UTF-8), 118–119
- unauthorized access, 412–414
- unauthorized tampering, 414–415
- unbind operation, 56, 87
- undo updates. *See* rollback.
- unique identifiers, replication, 386
- unique names. *See* DNs (distinguished names); unique identifiers.
- unit of replication, 375
- UNIX file system hierarchy *versus* LDAP directory hierarchy, 63–66
- unknownRequest() method, 721–722
- update-capable clients, data maintenance, 566–567
- update conflict resolution policy, 383–384
- update operations
 - add, 56, 82
 - delete, 56, 82
 - modify, 56, 84–86
 - modify DN (rename), 56, 83–84, 85
- update resolution policies, 389–391
- update statements, LDIF, 96–100
- updating directories, 56
- URLs of LDAP resources. *See* online resources.
- usage() function, 674–675
- user attributes, 62
- user-maintained data, 565–570
- user surveys, 573
- userid2dn() function, 681–682
- users
 - configuration and preference management, 28
 - as data source, 254
 - feedback from piloting, 492–494, 496–497
 - needs and expectations
 - accuracy and completeness, 221–222
 - versus* application needs, 223
 - asking your users, 220–221
 - determining your audience, 222–223
 - overview, 211
 - prioritizing, 223
 - privacy, 222
 - privacy needs definition, 423, 425–426
 - Using Digest Authentication as a SASL Mechanism* (RFC 2831), 140
 - UTF-8 (UCS Transformation Format 8), 118–119
 - utilities. *See* command-line utilities; setpwd utility; tools.
- value constraint plug-in example, 180–197
- values (of attributes). *See* attribute values.
- vendors
 - disaster recovery services, 549
 - evaluating directory services software, 472, 475–476
 - performance figures, 401
- verifying backups, 548–549
- vertical bar (|), OR operator within search filters, 78
- Virtual List View (VLV) Request control, 132–136
- Virtual List View (VLV) Response control, 132–136
- virtual directories, 770–773
- virtual networks, 459
- virtual synchronization, 770–773
- VLV (Virtual List View) Request control, 132–136
- VLV (Virtual List View) Response control, 132–136
- wall-clock time, replication, 385
- Web resources. *See* online resources.
- Web server information, organizing and accessing, 36–37
- Web servers *versus* directories, 33–34
- Web site with user profile storage, SimpleSite sample application, 687–722
- writeHrefButton() method, 720–721
- writePageFooter() method, 720–721
- writePageHeader() method, 720–721
- X.500 directory server software, 345–346
- X.500 specification, 38–41
- XML (eXtensible Markup Language), 143–145, 163–164