

Index

• A •

- A resource record, 57–59
- Abstract type category (object classes), 221–222
- Access Control Entry (ACE), 234, 305
- Access Control List (ACL), 234, 305
- access token, 234
- accidental deletions, 265
- Account Lockout Policy, 240, 248
- Account Operators Group, 194
- Account Policy, 240
- ACE (Access Control Entry), 234, 305
- ACL (Access Control List), 234, 305
- Active Directory (AD)
 - benefits, 22
 - defined, 7–10
 - Lightweight Directory Access Protocol (LDAP), 10
 - Microsoft Exchange Server V4.0 through V5.5 directory service, 10
 - popularity of, 1, 7
- Active Directory Application Mode (ADAM), 8, 130
- Active Directory Certificate Services (AD CS). *See* Certificate Services (CS)
- Active Directory Domain Services (AD DS). *See* Domain Services (DS)
- Active Directory Domain Services Installation Wizard, 303
- Active Directory Federation Services (AD FS). *See* Federation Services (FS)
- Active Directory Lightweight Directory Services (AD LDS). *See* Lightweight Directory Services (LDS)
- Active Directory namespace
 - defined, 62–63
 - naming conventions, 64–66
 - planning, 66–69
- Active Directory Rights Management Services (AD RMS). *See* Rights Management Services (RMS)
- Active Directory Schema snap-in, 220–221
- Active Directory Services Interface (ADSI), 306
- Active Directory sites. *See* sites
- Active Directory Users and Computers (ADUC) console, 175–178
- AD (Active Directory). *See* Active Directory (AD)
- AD CS (Active Directory Certificate Services). *See* Certificate Services (CS)
- AD DS (Active Directory Domain Services). *See* Domain Services (AD DS)
- AD LDS (Active Directory Lightweight Directory Services), 305. *See* Lightweight Directory Services (LDS)
- AD Preparation Wizard, 303
- AD RMS (Active Directory Rights Management Services), 306. *See* Rights Management Services (RMS)
- ADAM (Active Directory Application Mode), 8, 130
- ADAMSYNC command line tool, 132
- adding
 - attributes, 228–229
 - classes, 228–229
 - groups, 190–192
 - users, 175–178
- address resource records, 57–59
- administration
 - administrative boundaries, 74
 - delegating administrative authority, 81–82
 - delegating administrative control, 198–201
 - design, 274
 - Schema Administrators group, 19, 220–221, 288
- administrative modeling, 30–31
- Administrator user type, 192
- Administrators Group, 194

- ADPREP command line tool, 303
 - ADSI (Active Directory Services Interface), 306
 - ADSIEDIT console, 177
 - ADSIEdit console, 226, 228
 - ADUC (Active Directory Users and Computers) console, 175–178
 - Allowed RODC Password Replication Group, 193
 - American National Standards Institute (ANSI), 18, 306
 - ANSI (American National Standards Institute), 18, 306
 - API (application programming interface), 306
 - application partition
 - creating, 122
 - defined, 20, 61
 - Lightweight Directory Services (LDS), 134
 - application programming interface (API), 306
 - applications
 - distributed applications, 307
 - organizational unit (OU), 15
 - assigning
 - operations masters, 120
 - passwords to users, 176
 - asymmetric encryption, 158, 167–168
 - attended domain controller installation, 110–115
 - attributes
 - adding, 228–229
 - classes, 220, 224
 - creating, 223
 - deactivating, 229–230
 - defined, 16, 219–220, 306
 - defining, 223
 - list of, 222
 - object identifier (OID), 18, 222, 310
 - optional attributes, 19
 - reactivating, 229
 - attributeSchema object, 223
 - auditing
 - defined, 248–249
 - disabling, 250
 - enabling, 249–251
 - viewing audit entries, 251–252
 - viewing audit settings, 249
 - AUDITPOL command line tool, 249–250, 303
 - authentication
 - defined, 13, 234, 306
 - external users, 141–143
 - Kerberos, 233–237
 - Lightweight Directory Services (LDS), 132–133
 - localizing, 84
 - network authentication services, 20
 - NTLM, 233–235
 - authoritative restore, 264–265
 - authorization
 - defined, 234
 - Kerberos, 233–237
 - NTLM, 233–235
 - Auxiliary type category (object classes), 221–222
- B •**
- backup application software, 261
 - Backup Operators Group, 194
 - backups
 - database files, 261–263
 - Server Backup feature, 261–263
 - third-party backup applications, 261
 - Windows Server Backup tool, 261–263
 - bandwidth, 306
 - base schema, 220–221
 - benefits of Active Directory (AD), 22
 - best practices, 39–40, 51
 - bind redirection, 135
 - blocking inheritance in Group Policy Objects (GPOs), 242–243
 - blogs
 - Confessions of an IT Geek Blog, 283–284
 - Directory Services Team Blog, 281
 - Exchange Server Team Blog, 281
 - Windows Server Team Blog, 282
 - Bradner, Scott, *TCP/IP For Dummies*, 5th Edition, 212

branch office users, 289
 Brandon, Cameron, *TCP/IP For Dummies*, 21
 bridgehead server, 206, 306
 budget
 implementation plan, 42
 support, 274
 bulk administration tools, 178
 business assessment, 45
 business information
 environment, 25–31
 goals, 31–32
 justification for Active Directory, 24–25

• C •

CA (Certificate Authority). *See*
 Certificate Authority (CA)
 canonical name, 57, 306
 canonical name resource records, 57
 Cert Publishers Group, 193
 Certificate Authority (CA), 158–163
 Certificate Revocation List (CRL),
 159–160
 Certificate Service DCOM Access
 Group, 194
 Certificate Services (CS)
 defined, 9, 305
 deploying, 160
 Enterprise PKI (PKIView) tool,
 164–165, 288
 features, 161–162
 Online Responder Service (ORS), 160,
 163–165
 Web Enrollment, 163, 165
 certificates
 defined, 158, 307
 PKIView tool, 288
 troubleshooting, 288
 CERTREQ command line tool, 303
 CERTUTIL command line tool, 303
 child domains
 defined, 14, 306
 trees, 74–75
 circular logging, 256
 claims, 144–145, 306

classes
 adding, 228–229
 attributes, 220, 224
 deactivating, 229–230
 defined, 219–220, 310
 inheritance, 222–223
 reactivating, 229
 schema, 220–221
 Server, 224
 types of, 221–222
 User, 224–227
 classSchema object, 223–224
 CNAME resource record, 57
 COM+ partition set, 184–185
 command line tools
 ADAMSYNC, 132
 CERTREQ, 303
 CERTUTIL, 303
 CSVDE, 178, 303
 DCDIAG, 303
 DCPROMO, 254, 285, 303
 DFSCMD, 289
 DFSRADMIN, 289
 DNSCMD, 293–294
 DSACL, 303
 DSADD, 178, 303
 DSAMAIN, 269, 301–302
 DSDBUTIL, 303
 DSGET, 303
 DSMGMT, 303
 DSMOD, 303
 DSQUERY, 303
 DSRM, 303
 GPFIXUP, 303
 GPRESULT, 304
 GPUPDATE, 304
 KSETUP, 304
 KTPASS, 304
 LDIFDE, 135, 178, 228, 304
 LDP, 177, 304
 NET, 304
 NETDOM, 304
 NLTEST, 304
 NSLOOKUP, 304
 NTDSUTIL, 231, 260, 294–300
 RENDOM, 78, 304

command line tools (*continued*)

- REPADMIN / REPLSUMMARY, 288
- REPADMIN, 269, 288, 300–301
- TELNET, 286
- WBADMIN, 263
- W32TM, 286, 304
- Computer Configuration GPO, 238–239
- computers, as an organizational unit (OU), 80
- Confessions of an IT Geek Blog, 283–284
- configuration
 - Domain Services (DS), 107–109
 - Federation Services (FS), 155
- configuration partition
 - defined, 20
 - Lightweight Directory Services (LDS), 133–134
- configuration set, 135
- configuring non-Windows machine to become a security principal, 304
- connected sites, 87
- consolidation store, 131–132
- containers
 - defined, 306
 - nested containers, 310
 - organizational unit (OU), 15–16, 306
- contingency plan, 47–48
- costs
 - implementation plan, 42
 - site links, 87, 215–216, 306
 - support costs, 274
- conventions for naming
 - distinguished name (DN), 64–65, 307
 - fully qualified domain name (FQDN), 64, 308
 - NetBIOS names, 65–66
 - relative distinguished name (RDN), 311
 - user principal name (UPN), 65, 68–69, 314
- creating
 - application partition, 122
 - attributes, 223
 - domain controllers (DCs), 21
 - domains, 78
 - global catalog (GC), 120
 - group policies, 120, 244

- groups, 190–192
- organization unit (OU), 120
- organizational unit (OU), 197–198
- organizational unit (OU) structure, 80
- site link bridges, 216–217
- site links, 94–96, 212–214
- sites, 120, 208–209
- subnets, 120, 210–212
- users, 175–178
- credential caching, 100–102
- CRL (Certificate Revocation List), 159–160
- cross-link trusts, 307
- Cryptographic Operators Group, 194
- CS (Certificate Services)
 - defined, 9, 305
 - deploying, 160
 - Enterprise PKI (PKIView) tool, 164–165, 288
 - features, 161–162
 - installation, 161
 - Online Responder Service (ORS), 160, 163–165
 - Web Enrollment, 163, 165
- CSVDE command line tool, 178, 303
- customizing, 11



- DAP (Directory Access Protocol), 10
- data table, 307
- database files
 - backups, 261–263
 - database file, 253–256
 - defragmenting, 256–260, 307
 - locating, 255
 - restoring, 263–265
 - shadow copies, 267–269
 - snapshots, 267–269
 - specifying location of, 254
 - transaction log files, 253–256
- datastore, 307
- DCDIAG command line tool, 303
- DCPROMO command line tool, 254, 285, 303
- DCPROMO Wizard, 115–120

- DCs (domain controllers). *See* domain controllers (DCs)
- DDNS (Dynamic DNS), 59, 307
- deactivating objects, 229–230
- Default Domain Policy, 288
- default users and groups, 192–196
- defining
 - attributes, 223
 - sites, 92–93
- defragmenting, 256–260, 307
- delegating
 - administrative authority, 81–82
 - administrative control, 198–201
- Delegation of Control Wizard, 198–201
- deleting
 - group policies, 247
 - objects, 303
- demographics, 33
- Denied RODC Password Replication Group, 193
- deploying
 - Certificate Services (CS), 160
 - Domain Services (DS), 107–109
 - Federation Services (FS), 154
- design
 - administrators, 274
 - domains, 275
 - iterative nature of, 277
 - logical-first approach, 50
 - network topology, 276
 - physical structure, 84–85
 - physical-first approach, 49–50
 - site topology, 88, 207
- determining the number of trees, 71–72
- DFSCMD command line tool, 289
- DFSRADMIN command line tool, 289
- diagrams, 75–76
- digital certificates
 - defined, 307
 - PKIView tool, 288
 - troubleshooting, 288
- digital rights management (DRM), 165
- digital signature, 158
- directory, 307
- Directory Access Protocol (DAP), 10
- Directory Information Shadowing Protocol (DISP), 10
- directory namespace. *See* namespace
- directory objects. *See* objects
- Directory Operational Binding Management Protocol (DOP), 10
- directory schema. *See* schema
- Directory Services Restore Mode (DSRM), 258–259
- Directory Services Team Blog, 281
- Directory System Protocol (DSP), 10
- directory-aware applications, 84–85
- disabling
 - auditing, 250
 - group policies, 247
- DISP (Directory Information Shadowing Protocol), 10
- distinguished name (DN), 64–65, 307
- distributed applications, 307
- Distributed DCOM Users Group, 195
- distribution groups, 188
- DLL file, registering, 220–221
- DN (distinguished name), 64–65, 307
- DNS (Domain Name Service)
 - advantages of using, 275
 - background loading of zone data, 70
 - defined, 21, 307
 - DNS namespace, 21–22, 63
 - DNS table, 56, 307
 - dynamic updates, 59
 - incremental zone transfers, 62
 - IPv6 support, 69
 - Lightweight Directory Services (LDS), 130
 - locator service, 56
 - name resolution, 56
 - need for, 55–56
 - read-only Domain Controller (RODC) support, 70
 - requirements, 57–59
 - resource records, 56–59, 311
 - running DNS on an RODC, 98–99
 - troubleshooting, 304
 - zones, 59–62, 70
- DNS namespace, 21–22, 63
- DNS table, 56, 307
- DnsAdmins Group, 193
- DNSSCMD command line tool, 293–294
- DnsUpdateProxy Group, 193

- document protection, 168–171
- documentation, 43, 45–49
- Domain Admins Group, 193
- Domain Computers Group, 193
- domain controllers (DCs)
 - attended domain controller
 - installation, 110–115
 - Configuration Partition, 20
 - creating, 21
 - database files, 253–256
 - defined, 13, 19, 85, 307
 - Domain Naming Partition, 19
 - global catalog (GC), 21
 - global catalog servers, 85–86
 - installation, 110–118
 - Lightweight Directory Services (LDS), 130
 - network authentication services, 20
 - optimizing disk performance, 255
 - placement of, 88–90, 277
 - promotion, 285
 - schema, 20
 - security, 84
 - Server Core, 107, 118
 - SYSVOL directory, 238, 253
 - troubleshooting, 285, 289, 303
 - unattended domain controller
 - installation, 116–118
- Domain Controllers Group, 193
- Domain Guests Group, 193
- domain local groups, 189
- Domain Name Service (DNS)
 - advantages of using, 275
 - background loading of zone data, 70
 - defined, 21, 307
 - DNS namespace, 21–22, 63
 - DNS table, 56, 307
 - dynamic updates, 59
 - incremental zone transfers, 62
 - IPv6 support, 69
 - Lightweight Directory Access Protocol (LDAP), 130
 - locator service, 56
 - name resolution, 56
 - need for, 55–56
 - read-only Domain Controller (RODC)
 - support, 70
 - requirements, 57–59
 - resource records, 56–59, 311
 - running DNS on an RODC, 98–99
 - troubleshooting, 304
 - zones, 59–62, 70
 - domain naming master, 91
- Domain Naming Partition, 19
- Domain Services (DS)
 - configuration, 107–109
 - defined, 8, 305
 - deploying, 107–109
 - installing from media, 122–123
 - Server Core, 106–107, 118–119, 312
 - stopping, 266
- domains
 - administrative boundaries, 74
 - child domain, 14, 306
 - child domains, 74–75
 - creating, 78
 - Default Domain Policy, 288
 - defined, 12–13, 307
 - design, 275
 - domain controller, 13
 - explicit trusts, 15
 - forests, 15, 72–73
 - functional level settings, 114
 - Lightweight Directory Services (LDS), 130
 - logon, 286–287
 - moving, 78
 - namespace, 14
 - organizational unit (OU), 15–17, 79
 - parent (root) domain, 14, 73–74, 311
 - password policies, 12, 73
 - renaming, 78, 304
 - replication, 13
 - root (parent) domain, 14, 73–74, 311–312
 - subdomains, 14, 313
 - transitive trust relationships, 14
 - trees, 13–15
 - trusts, 14–15
- DOP (Directory Operational Binding Management Protocol), 10
- DRM (digital rights management), 165

DS (Domain Services)
 configuration, 107–109
 defined, 8, 305
 deploying, 107–109
 installing from media, 122–123
 Server Core, 106–107, 118–119, 312
 stopping, 266
DSACL command line tool, 303
DSADD command line tool, 178, 303
DSAMAIN command line tool, 269,
 301–302
DSDBUTIL command line tool, 303
DSGET command line tool, 303
DSMGMT command line tool, 303
DSMOD command line tool, 303
DSP (Directory System Protocol), 10
DSQUERY command line tool, 303
DSRM command line tool, 303
DSRM (Directory Services Restore
 Mode), 258–259
Dynamic DNS (DDNS), 59, 307
dynamic updates, 59

• E •

editing
 group policies, 245–246
 groups, 190–192
 user attributes, 178–183
editions of Windows Server 2008,
 104–105
enabling auditing, 249–251
encryption
 asymmetric encryption, 158, 167–168
 symmetric encryption, 158, 167
end-user trainers (for implementation
 planning team), 44
Enterprise Admins Group, 73, 194
Enterprise PKI (PKIView) tool,
 164–165, 288
Enterprise Read-only Domain
 Controllers Group, 194
errors, monitoring, 287
ESE (Extensible Storage Engine),
 253, 308
Event Log Policy, 240
Event Log Users Group, 195

Event Viewer tool, 267, 287
Exchange Server Team Blog, 281
Exchange Server V4.0 through V5.5
 directory service, 10
executive sponsor (on implementation
 planning team), 44
explicit trusts, 15, 307
extending schema, 18–19, 227–228
extensibility, 11, 308
Extensible Storage Engine (ESE),
 253, 308
external trusts, 308
external users and authentication,
 141–143

• F •

failed AD implementations, 23–24
fault tolerance, 308
Federation Services (FS)
 configuration, 155
 defined, 9, 147, 305
 deploying, 154–155
 federated Web single sign-on (SSO)
 scenario, 150–152
 federated Web single sign-on (SSO)
 with forest trust scenario, 152–153
 Federation Service Proxy, 154
 how it works, 147–148
 software requirements, 155
 Web Agent, 154
 Web single sign-on scenario, 149–150
federations
 claims, 144–145, 306
 defined, 143, 146, 308
 identities, 144
 security token services, 145–146
 tokens, 144–145, 313
file shares, as an organizational unit
 (OU), 15, 80
File System Policy, 240
Flexible Single Master Operations
 (FSMO). *See* Operations Masters
forcing
 remote shutdowns, 304
 replication, 311
forest-level trusts, 79

- forests. *See also* trees
 - defined, 15, 72, 308
 - domains, 72–73
 - functional level settings, 114
 - global catalog (GC), 73
 - Lightweight Directory Services (LDS), 130
 - multiple forests model, 78
 - namespace, 71–72
 - scope, 274–275
 - FQDN (fully qualified domain name), 64, 308
 - fragmentation, 308
 - frequency of garbage collection, 258
 - frequency value of site links, 87, 96
 - FS (Federation Services)
 - configuration, 155
 - defined, 9, 147, 305
 - deploying, 154–155
 - federated Web single sign-on (SSO) scenario, 150–152
 - federated Web single sign-on (SSO) with forest trust scenario, 152–153
 - Federation Service Proxy, 154
 - how it works, 147–148
 - software requirements, 155
 - Web Agent, 154
 - Web single sign-on scenario, 149–150
 - FSMO (Flexible Single Master Operations). *See* Operations Masters
 - fully qualified domain name (FQDN), 64, 308
 - functional level settings, 114
 - functional modeling, 76–78, 308
 - functional specification, 46–47
 - functional view (of a business), 27–28
- **G** •
- gap analysis, 46
 - garbage collection, 258, 308
 - gathering information. *See* information gathering
 - GC (global catalog). *See* global catalog (GC)
 - geographic modeling, 28–29, 76–77, 309
 - Global Address List, 84–85
 - global catalog (GC)
 - creating, 120
 - defined, 21, 85, 309
 - forests, 73
 - Lightweight Directory Services (LDS), 130
 - global catalog servers
 - domain controllers (DCs), 85–86
 - placement of, 90, 277
 - global groups, 189
 - GlobalNames zone (DNS), 70
 - goals
 - business goals, 31
 - implementation plan, 42
 - technical goals, 39
 - GPFIXUP command line tool, 303
 - GPMC (Group Policy Management Console), 244
 - GPO (Group Policy Object). *See* group policies
 - GPRESULT command line tool, 304
 - GPUPDATE command line tool, 304
 - group policies
 - Account, 240
 - Account Lockout Policy, 240, 248
 - blocking inheritance, 242–243
 - creating, 120, 244
 - defined, 309
 - deleting, 247
 - disabling, 247
 - editing, 245–246
 - Event Log Policy, 240
 - File System Policy, 240
 - implementing, 237–239
 - inheritance, 240–243
 - IP Security Policy, 240
 - Kerberos Policy, 240
 - Lightweight Directory Services (LDS), 130
 - linking, 246–247
 - Local Policy, 240
 - managing, 244
 - modeling, 248
 - naming, 244
 - Password Policy, 240, 248

- Public Key Policy, 240
 - Registry Policy, 240
 - reinstating, 247
 - reporting, 248
 - Restricted Groups Policy, 240
 - Resultant Set of Policy (RSOP), 248
 - security, 239–240
 - starter GPO, 245
 - System Services Policy, 240
 - troubleshooting, 289
 - Group Policy Creator Owners Group, 194
 - Group Policy Management Console (GPMC), 244
 - Group Policy Management Editor, 239
 - Group Policy Object (GPO). *See* group policies
 - groups
 - Account Operators Group, 194
 - adding, 190–192
 - Administrators Group, 194
 - Allowed RODC Password Replication Group, 193
 - Backup Operators Group, 194
 - Cert Publishers Group, 193
 - Certificate Service DCOM Access, 194
 - creating, 190–192
 - Cryptographic Operators Group, 194
 - default groups, 192–196
 - Denied RODC Password Replication Group, 193
 - Distributed DCOM Users, 195
 - distribution groups, 188
 - DnsAdmins Group, 193
 - DnsUpdateProxy Group, 193
 - Domain Admins Group, 193
 - Domain Computers Group, 193
 - Domain Controllers Group, 193
 - Domain Guests Group, 193
 - domain local groups, 189
 - editing, 190–192
 - Enterprise Admins, 73, 194
 - Enterprise Read-only Domain Controllers Group, 194
 - Event Log Users Group, 195
 - global groups, 189
 - Group Policy Creator Owners, 194
 - Guests Group, 195
 - IIS_IUSRS, 195
 - Incoming Forest Trust Builders Group, 195
 - Network Configuration Operators Group, 195
 - organizational unit (OU), 15, 79
 - Performance Log Users Group, 195
 - policy settings, 289
 - Print Operators Group, 196
 - RAS and IAS Servers Group, 193
 - Read-only Domain Controllers Group, 194
 - Remote Desktop Users Group, 196
 - Replicator Group, 196
 - Schema Administrators group, 19, 220–221, 288
 - Schema Admins Group, 194
 - security groups, 188
 - Server Operators Group, 196
 - Terminal Server License Servers Group, 196
 - universal group caching, 85
 - universal groups, 189
 - users, 185–189
 - Users Group, 196
 - Windows Authorization Access Group, 196
 - Guest user type, 192
 - Guests Group, 195
- H ●
- hash, 102, 158
 - Health Insurance Portability and Accountability Act (HIPAA), 165
 - hierarchies
 - Certificate Authority (CA), 162–163
 - defined, 11, 309
 - logical, 11–12, 310
 - organizational units (OUs), 16
 - physical, 11–12, 311
 - HIPAA (Health Insurance Portability and Accountability Act), 165
 - home share, 181
 - Hyper-V, 105

• I •

identity, 144–145

Identity Integration Feature Pack (IIFP), 131–132

Identity Lifecycle Manager (ILM), 130, 132

identity management needs, 276

IETF (Internet Engineering Task Force), 58, 309

IIS_IUSRS Group, 195

ILM (Identity Lifecycle Manager), 130, 132

implementation plan

- best practices, 51
- budget, 42
- business assessment, 45
- contingency plan, 47–48
- documentation, 43, 45–49
- functional specification, 46–47
- gap analysis, 46
- goals, 42
- implementation standards, 47
- information gathering, 43
- need for, 41–42, 273–274
- personnel, 42
- requirements/scope document, 45–46
- risk, 42, 47–48
- schedule, 42, 48–49
- scope, 45–46
- team, 43–44
- technical assessment, 45
- tracking, 48–49
- training, 42
- vision statement, 45

implementing group policies, 237–239

Incoming Forest Trust Builders Group, 195

incremental zone transfers, 62

information gathering

- business information, 24, 26–32
- implementation plan, 43
- importance of, 23–24
- technical information, 32–39

information store, 9–11

information usage

- digital rights management (DRM), 165
- managing, 165–166

infrastructure master, 91

inheritance

- defined, 309
- Group Policy Object (GPO), 240–243
- object classes, 222–223

Initial Configuration Tasks Wizard, 107–108

installation

- Certificate Services (CS), 161
- defined, 309
- domain controllers (DCs), 110–118
- Domain Services (DS), 122–124
- Lightweight Directory Services (LDS), 136–139
- read-only domain controllers (RODCs), 124–125
- Rights Management Services (RMS), 172
- Windows Server 2008, 103–107

instance

- defined, 309
- Lightweight Directory Services (LDS), 133–135

Internet Drafts, 58

Internet Engineering Task Force (IETF), 58, 309

Internet Protocol (IP), 309

intersite replication, 205–206, 309

intrasite replication, 204–205, 309

IP (Internet Protocol), 309

IP Security Policy, 240

IPv6 support (DNS software), 69

IT support trainers (for implementation planning team), 44

iterative nature of design, 277

• K •

Kerberos

- Authentication Service (AS), 236
- defined, 233–234, 309
- features, 235–237
- key, 236
- Key Distribution Center (KDC), 20, 236, 310
- Lightweight Directory Services (LDS), 129
- shared secret, 236

Ticket-Granting Service (TGS), 236
time synchronization, 286
Kerberos Policy, 240
key, 236
keys
 defined, 158
 private key, 167
 public key, 167
krbtgt user type, 192
KSETUP command line tool, 304
KTPASS command line tool, 304



LAN (local area network), 13
LDAP Delimited Interchange Format (LDIF) files, 139–140
LDAP (Lightweight Directory Access Protocol), 10, 310
LDIF (LDAP Delimited Interchange Format) files, 139–140
LDIFDE command line tool, 135, 178, 228, 304
LDP command line tool, 177, 304
LDS (Lightweight Directory Services)
 application partition, 134
 authentication, 132–133
 bind redirection, 135
 configuration partition, 133–134
 configuration set, 135
 consolidation store, 131–132
 defined, 305
 domain controllers (DCs), 130
 Domain Name Service (DNS), 130
 domains, 130
 forests, 130
 global catalog (GC), 130
 group policies, 130
 installation, 136–139
 instance, 133–135
 Kerberos, 129
 LDIF (LDAP Delimited Interchange Format) files, 139–140
 partitions, 133–134
 phone book service, 131
 replication, 135–136
 schema partition, 133–134

 security, 135
 site links, 130
 sites, 130
 subnets, 130
 X.500 directory service standard, 133
lead design architect (on implementation planning team), 44
leaf, 310
Leiden, Candance, *TCP/IP For Dummies*, 5th Edition, 212
lifetime of tombstone, 257–258
Lightweight Directory Access Protocol (LDAP), 10, 310
Lightweight Directory Services (LDS)
 application partition, 134
 authentication, 132–133
 bind redirection, 135
 configuration partition, 133–134
 configuration set, 135
 consolidation store, 131–132
 defined, 8, 305
 domain controllers (DCs), 130
 Domain Name Service (DNS), 130
 domains, 130
 forests, 130
 global catalog (GC), 130
 group policies, 130
 installation, 136–139
 instance, 133–135
 Kerberos, 129
 LDIF (LDAP Delimited Interchange Format) files, 139–140
 partitions, 133–134
 phone book service, 131
 replication, 135–136
 schema partition, 133–134
 security, 135
 site links, 130
 sites, 130
 subnets, 130
 X.500 directory service standard, 133
linking group policies, 246–247
local area network (LAN), 13
Local Policy, 240
localizing authentication, 84
location of database files, 254–255
locator service, 56

- log files, 253–256
- logical structure, 11–12, 310
- logical-first approach to design, 50
- logon
 - domain, 286–287
 - Single Sign-on (SSO) service, 9

• M •

- mail exchange resource records, 57
- managing
 - group policies, 244
 - information usage, 165–166
 - trusts, 304
- metadata, 219
- Microsoft
 - Directory Services Team Blog, 281
 - Exchange Server Team Blog, 281
 - Exchange Server V4.0 through V5.5
 - directory service, 10
 - Identity Integration Feature Pack (IIFP), 131–132
 - Identity Lifecycle Manager (ILM), 130, 132
 - TechNet Magazine Web site, 280
 - Windows Server 2008 RSS feeds, 283
 - Windows Server 2008 TechCenter Web site, 280
 - Windows Server 2008 Web site, 279–280
 - Windows Server Team Blog, 282
- Microsoft Identity Integration Server (MIIS), 130
- Microsoft Management Console (MMC), 21
- mixed mode, 114, 310
- modeling
 - administrative modeling, 30–31
 - functional modeling, 76–78, 308
 - geographic modeling, 28–29, 76, 309
 - group policies, 248
 - multiple forests model, 78–79
- modifying
 - Default Domain Policy, 288
 - frequency of garbage collection, 258
 - objects, 303
 - schema, 18–19, 227–228, 276, 288
 - user attributes, 178–183

- monitoring, 287
- moving domains, 78
- MS-AdamSyncMetadata LDIF file, 140
- MS-ADLDS-DisplaySpecifiers LDIF file, 140
- MS-AZMan LDIF file, 140
- MS-InetOrgPerson LDIF file, 140
- MS-User LDIF file, 140
- MS-UserProxy LDIF file, 140
- MS-UserProxyFull LDIF file, 140
- multimaster model, 20
- multimaster replication, 204
- multiple forests model, 79
- MX resource record, 57

• N •

- name resolution, 56
- name server resource records, 57
- namespace
 - Active Directory namespace, 62–69
 - defined, 14, 62–63, 310
 - DNS namespace, 21–22, 63
 - forests, 71–72
 - trees, 71–72
 - WINS (Windows Internet Naming Server), 70
- naming
 - group policies, 244
 - organizational unit (OU), 197
 - site link bridges, 217
 - site links, 213
 - sites, 208–209
- naming conventions
 - distinguished name (DN), 64–65, 307
 - fully qualified domain name (FQDN), 64, 308
 - NetBIOS names, 65–66
 - relative distinguished name (RDN), 311
 - user principal name (UPN), 65, 68–69, 314
- native mode, 114, 310
- nesting
 - containers, 310
 - organizational units (OUs), 16–17, 80
- NET command line tool, 304
- NetBIOS names, 65–66

- NETDOM command line tool, 304
 - network authentication services, 20
 - Network Configuration Operators Group, 195
 - network topology, 276, 313
 - networks
 - fault tolerance, 308
 - infrastructure, 34–37
 - locator service, 56
 - traffic, 87, 214–215
 - troubleshooting, 286
 - NLTEST command line tool, 304
 - non-authoritative restore, 263–264
 - nontransitive trusts, 310
 - non-Windows machine, configuring to become a security principal, 304
 - NS resource record, 57
 - NSLOOKUP command line tool, 304
 - NTDS.DIT file, 220, 254
 - NTDSUTIL command line tool
 - Activate Instance command, 260, 295–296
 - Authoritative Restore command, 296
 - Compact To command, 260
 - Files command, 260, 296–297
 - IFM command, 297–298
 - Info command, 260
 - Local Roles command, 298–299
 - offline defragmentation, 260
 - Roles command, 299
 - running, 294–300
 - Set DSRM Password command, 299–300
 - Snapshot command, 300
 - transferring schema master role, 231
 - NTLM authentication/authorization protocol, 233–235
- ○ ●
- object attributes
 - adding, 228–229
 - creating, 223
 - deactivating, 229–230
 - defined, 16, 219–220, 306
 - defining, 223
 - list of, 222
 - object classes, 220
 - object identifier (OID), 18, 222, 310
 - optional attributes, 19
 - reactivating, 229
 - object classes
 - adding, 228–229
 - attributes, 220, 224
 - deactivating, 229–230
 - defined, 219–220, 310
 - inheritance, 222–223
 - reactivating, 229
 - schema, 220–221
 - Server, 224
 - types of, 221–222
 - User, 224–227
 - object identifier (OID), 18, 222, 310
 - objects
 - attributeSchema, 223
 - classSchema, 223–224
 - customizing, 11
 - deactivating, 229–230
 - defined, 11, 16, 219–220, 310
 - deleting, 303
 - distinguished name (DN), 64–65
 - extensibility, 11
 - fully qualified domain name (FQDN), 64
 - global catalog (GC), 21, 309
 - Group Policy Object (GPO), 309
 - hierarchy, 11–12
 - leaf, 310
 - modifying, 303
 - organizational units (OUs), 15–16
 - reactivating, 229
 - retrieving properties of, 303
 - schema, 219–221
 - tombstone, 256–258, 313
 - types of, 221–222
 - offline defragmenting, 256–260
 - OID (object identifier), 18, 222, 310
 - Online Certificate Status Protocol (OSCP), 164
 - online defragmenting, 256–259
 - Online Responder Service (ORS), 160, 163–165

- operations masters
 - assigning, 120
 - defined, 311
 - domain naming master, 91
 - Flexible SingleMaster Operations (FSMOs), 90
 - infrastructure master, 91
 - PDC emulator, 91
 - placement of, 90–92
 - RID master, 91
 - schema master, 90, 230–231
- optimizing disk performance of domain controller, 255
- optional attributes, 19
- organizational unit (OU)
 - applications, 15
 - computers, 80
 - containers, 306
 - creating, 120, 197–198
 - creating OU structure, 80
 - defined, 15, 79, 311
 - domains, 79
 - file shares, 15, 80
 - groups, 15, 79
 - hierarchy, 16
 - naming, 197
 - nesting OUs, 16–17, 80
 - printers, 15, 80
 - users, 15, 79
- organizational view (of a business), 27
- ORS (Online Responder Service), 160, 163–165
- OSCP (Online Certificate Status Protocol), 164
- OU (organizational unit)
 - applications, 15
 - computers, 80
 - containers, 306
 - creating, 120, 197–198
 - creating OU structure, 80
 - defined, 15, 79, 311
 - domains, 79
 - file shares, 15, 80
 - groups, 15, 79
 - hierarchy, 16
 - naming, 197
 - nesting OUs, 16–17, 80
 - printers, 15, 80
 - users, 15, 79
- parent (root) domain
 - defined, 14, 311–312
 - trees, 73–74
- parent-child trusts, 311
- partitions
 - application partitions, 20, 61, 122
 - Configuration Partition, 20
 - defined, 311
 - Domain Naming Partition, 19
 - Lightweight Directory Services (LDS), 133–134
 - multimaster model, 20
 - replication, 20
 - schema, 20
- password policies, 12, 73, 240, 248
- passwords, assigning to users, 176–177
- PDC emulator, 91
- Performance Log Users Group, 195
- performance monitoring, 287
- personnel, as part of implementation plan, 42
- phone book service, 131
- physical structure
 - defined, 11–12, 311
 - design, 84–85
- physical-first approach to design, 49–50
- PING, 286
- PKI (public key infrastructure), 157–158
- PKIView tool, 288
- placement
 - of domain controllers (DCs), 88–90, 277
 - of global catalog servers, 90, 277
 - of operations masters, 90–92
- planning for implementation
 - best practices, 51
 - budget, 42
 - business assessment, 45
 - contingency plan, 47–48
 - documentation, 43, 45–49
 - functional specification, 46–47



- gap analysis, 46
 - goals, 42
 - implementation standards, 47
 - information gathering, 43
 - need for, 41–42, 273–274
 - personnel, 42
 - requirements/scope document, 45–46
 - risk, 42, 47–48
 - schedule, 42, 48–49
 - scope, 45–46
 - team, 43–44
 - technical assessment, 45
 - tracking, 48–49
 - training, 42
 - vision statement, 45
 - pointer resource records, 57
 - policies
 - Account, 240
 - Account Lockout Policy, 240, 248
 - blocking inheritance, 242–243
 - creating, 120, 244
 - defined, 309
 - deleting, 247
 - disabling, 247
 - editing, 245–246
 - Event Log Policy, 240
 - File System Policy, 240
 - implementing, 237–239
 - inheritance, 240–243
 - IP Security Policy, 240
 - Kerberos Policy, 240
 - Lightweight Directory Services (LDS), 130
 - linking, 246–247
 - Local Policy, 240
 - managing, 244
 - modeling, 248
 - naming, 244
 - Password Policy, 240, 248
 - Public Key Policy, 240
 - Registry Policy, 240
 - reinstating, 247
 - reporting, 248
 - Restricted Groups Policy, 240
 - Resultant Set of Policy (RSOP), 248
 - security, 239–240
 - starter GPO, 245
 - System Services Policy, 240
 - troubleshooting, 289
 - popularity of Active Directory, 1, 7
 - preventing accidental deletions, 265
 - primary zones (DNS), 60
 - Print Operators Group, 196
 - printers, as an organizational unit (OU), 15, 80
 - private key, 167
 - project manager, 44
 - project owner, 31–32
 - promotion of domain controllers (DCs), 285
 - propagating updates, 206–207, 311
 - protocols
 - Directory Access Protocol (DAP), 10
 - Directory Information Shadowing Protocol (DISP), 10
 - Directory Operational Binding Management Protocol (DOP), 10
 - Directory System Protocol (DSP), 10
 - Internet Protocol (IP), 309
 - Kerberos authentication/authorization protocol, 233–234
 - Lightweight Directory Access Protocol (LDAP), 10
 - NTLM authentication/authorization protocol, 233–235
 - Online Certificate Status Protocol (OSCP), 164
 - Simple Mail Transport Protocol (SMTP), 87
 - TCP/IP, 21
 - X.500, 10
 - provisioning, 130
 - PTR resource record, 57
 - public key, 167
 - public key infrastructure (PKI), 157–158
 - Public Key Policy, 240
- R •**
- RAS and IAS Servers Group, 193
 - RDN (relative distinguished name), 311
 - reactivating objects, 229

- Read-only Domain Controllers Group, 194
- read-only domain controllers (RODCs)
 - administrative separation, 99–100
 - credential caching, 100–102
 - defined, 20, 96–97, 311
 - DNS support, 70
 - installation, 124–125
 - limitations, 97–98
 - prerequisites, 97–98
 - running DNS on an RODC, 98–99
 - troubleshooting, 289
- Really Simple Syndication (RSS)
 - feeds, 283
- recovering snapshots, 269
- regions (partitions)
 - application partitions, 20, 61
 - Configuration Partition, 20
 - Domain Naming Partition, 19
 - multimaster model, 20
 - replication, 20
 - schema, 20
- registering
 - DLL file, 220–221
 - Schema snap-in, 220–221
- Registry Policy, 240
- regsvr32 utility, 220
- reinstating group policies, 247
- relative distinguished name (RDN), 311
- Relative Identifier (RID), 91
- Reliability and Performance Monitor
 - tool, 287
- reloading schema cache, 231–232
- remote access, 185–186
- Remote Desktop Users Group, 196
- renaming domains, 78, 304
- RENDOM command line tool, 78, 304
- REPADMIN / REPLSUMMARY
 - command, 288
- REPADMIN command line tool, 269, 288, 300–301
- replication *See also* Updates
 - defined, 13, 311
 - forcing, 311
 - intersite replication, 205–206, 309
 - intrasite replication, 204–205, 309
 - Lightweight Directory Services (LDS), 135–136
 - multimaster replication, 204
 - partitions, 20
 - REPADMIN command line tool, 269, 288, 300–301
 - traffic, 84
 - troubleshooting, 288
- replication latency, 232, 311
- Replicator Group, 196
- reporting for group policies, 248
- Request for Comments (RFC), 58
- required attributes, 19
- requirements/scope document, 45–46
- resource monitoring, 287
- resource records, 56–59, 311
- restarting, 265–266
- restoring Active Directory
 - accidental deletions, 265
 - authoritative restore, 264–265
 - non-authoritative restore, 263–264
- Restricted Groups Policy, 240
- Resultant Set of Policy (RSoP), 248, 289
- retrieving properties of objects, 303
- RFC (Request for Comments), 58
- RID master, 91
- RID (Relative Identifier), 91
- Rights Management Services (RMS)
 - asymmetric encryption, 167–168
 - defined, 9, 166, 306
 - document protection, 168–171
 - installation, 172
 - offline access, 170
 - online access, 170
 - symmetric encryption, 167
- risk, 42, 47–48
- RMS (Rights Management Services)
 - asymmetric encryption, 167–168
 - defined, 9, 166, 306
 - document protection, 168–171
 - installation, 172
 - offline access, 170
 - online access, 170
 - symmetric encryption, 167

- RODCs (read-only domain controllers)
 - administrative separation, 99–100
 - credential caching, 100–102
 - defined, 20, 96–97, 311
 - DNS support, 70
 - installation, 124–125
 - limitations, 97–98
 - prerequisites, 97–98
 - running DNS on an RODC, 98–99
 - troubleshooting, 289
 - root (parent) domain
 - defined, 14, 311–312
 - trees, 73–74
 - RSoP (Resultant Set of Policy), 248, 289
 - RSS (Really Simple Syndication)
 - feeds, 283
 - running DNS on an RODC, 98–99
- S •**
- safe mode, 312
 - SAM (Security Accounts Manager), 312
 - Sarbanes-Oxley Act, 165
 - scalability, 25
 - scheduling
 - implementation plan, 42, 48–49
 - network traffic, 87, 214–215
 - snapshots, 268
 - schema
 - attributes, 219–220
 - base schema, 220–221
 - defined, 18, 219, 312
 - definitions, 219–220
 - domain controllers (DCs), 20
 - extending, 18–19, 227–228
 - Lightweight Directory Services (LDS), 133–134
 - metadata, 219
 - modifying, 18–19, 227–228, 276, 288
 - NTDS.DIT file, 220
 - objects, 219–221
 - schema master, 90, 230–231
 - schema policy, 47
 - troubleshooting, 288
 - viewing, 220–221, 226
 - Schema Administrators group, 19, 220–221, 288
 - Schema Admins Group, 194
 - schema cache
 - defined, 312
 - reloading, 231–232
 - updates, 231–232
 - Schema snap-in, 220–221
 - scope
 - forest, 274–275
 - implementation plan, 45–46
 - secondary zones (DNS), 60
 - security
 - domain controllers (DCs), 84
 - group policies, 239–240
 - Lightweight Directory Services (LDS), 135
 - public key infrastructure (PKI), 157–158
 - security standards, 47
 - Security Accounts Manager (SAM), 312
 - security groups, 188
 - Security Identifier (SID), 91, 234, 312
 - security token services, 145–146
 - security vulnerabilities, 233
 - seizing schema master role, 231
 - Server Backup feature, 261–263
 - Server Core, 106–107, 118–119, 312
 - Server Manager tool, 109
 - Server object class, 224
 - Server Operators Group, 196
 - server visualization technology, 105
 - servers
 - bridgehead server, 206, 306
 - canonical name, 57
 - forcing remote shutdowns, 304
 - service resource records, 57–59
 - session ticket, 312
 - shadow copies, 267–269
 - shared secret, 236
 - shutdowns, forcing remote
 - shutdowns, 304
 - SID (Security Identifier), 91, 234, 312
 - Simple Mail Transport Protocol (SMTP), 87

- Single Sign-on (SSO), 9, 143
 - site link bridges, 87, 207, 216–217, 312
 - site links
 - connected sites, 87
 - costs, 87, 215–216, 306
 - creating, 94–96, 212–214
 - defined, 16–17, 87, 207, 312
 - frequency value, 87, 96
 - Lightweight Directory Services (LDS), 130
 - naming, 213
 - Simple Mail Transport Protocol (SMTP), 87
 - transitive site links, 214
 - site topology, 88, 207
 - sites
 - creating, 120, 208–209
 - defined, 16–17, 86, 207, 312
 - defining, 92–93
 - Lightweight Directory Services (LDS), 130
 - naming, 208–209
 - SMTP (Simple Mail Transport Protocol), 87
 - snapshots, 267–269
 - SOA resource record, 57
 - specifying location of database files, 254
 - SRV resource record, 57–59
 - SSO (Single Sign-on), 9, 143
 - start of authority resource records, 57
 - starter GPO, 245
 - stopping Active Directory Domain Services (AD DS), 266
 - Structural type category (object classes), 221–222
 - structure of objects
 - defined, 11
 - logical structure, 11–12, 310
 - organizational units (OUs), 16
 - physical structure, 11–12, 311
 - stub zones (DNS), 60–61
 - subdomains, 14, 313
 - subject matter experts (on implementation planning team), 44
 - subnets
 - creating, 120, 210–212
 - defined, 86–87, 313
 - Lightweight Directory Services (LDS), 130
 - support costs, 274
 - symmetric encryption, 158, 167
 - synchronization, 313
 - System Services Policy, 240
 - SYSVOL directory, 238, 253
- T ●
- TCP/IP, 21
 - TCP/IP For Dummies* (Brandon), 21
 - TCP/IP For Dummies*, 5th Edition (Leiden, Wilensky, and Bradner), 212
 - team for implementation plan, 43–44
 - TechNet Magazine Web site, 280
 - technical assessment, 45
 - technical information, 32–39
 - TELNET command, 286
 - Terminal Server License Servers Group, 196
 - Terminal Services, 182–184, 187–188
 - testers (on implementation planning team), 44
 - TGS (Ticket-Granting Service), 236
 - TGT (Ticket Granting Ticket), 96, 236–237, 313
 - third-party backup applications, 261
 - Ticket Granting Ticket (TGT), 96, 236–237, 313
 - Ticket-Granting Service (TGS), 236
 - time synchronization, 286
 - time zone, 107
 - tokens
 - defined, 144–145, 313
 - security token services, 145–146
 - tombstone, 256–258, 313
 - topology, 276, 313
 - tracking implementation plan, 48–49
 - training, 42
 - transaction log files, 253–256
 - transitive site links, 214
 - transitive trusts, 14, 313

- tree-root trusts, 313
 - trees. *See also* forests
 - child domains, 74–75
 - defined, 13–15, 72, 313
 - determining the number of, 71–72
 - diagrams, 75–76
 - namespace, 71–72
 - root (parent) domain, 73–74
 - troubleshooting
 - branch office users, 289
 - certificates, 288
 - domain controller promotion, 285
 - domain controllers (DCs), 285, 289, 303
 - domain logon, 286–287
 - Domain Name Service (DNS), 304
 - Event Viewer tool, 267, 287
 - group policies, 289
 - network issues, 286
 - policy settings, 289
 - read-only Domain Controller (RODC), 289
 - Reliability and Performance Monitor tool, 287
 - replication, 288
 - schema, 288
 - time synchronization, 286
 - Windows Time Service, 304
 - trusts
 - cross-link, 307
 - defined, 75, 313
 - explicit, 15, 307
 - external, 308
 - forest-level, 79
 - managing, 304
 - nontransitive, 310
 - parent-child, 311
 - transitive, 14, 313
 - tree-root, 313
 - verifying, 304
 - viewing, 304
 - types of classes, 221–222
- **U** •
- unattended domain controller
 - installation, 115–118
 - universal group caching, 85, 121
 - universal groups, 189
 - updates. *See also* replication
 - propagating, 206–207, 311
 - schema cache, 231–232
 - UPN (user principal name), 65, 68–69, 314
 - User Configuration GPO, 238–239
 - User object class, 224–227
 - user principal name (UPN), 65, 68–69, 314
 - users
 - adding, 175–178
 - Administrator, 192
 - branch office users, 289
 - bulk administration tools, 178
 - COM+ partition set, 184–185
 - creating, 175–178
 - default users, 192
 - editing attributes, 178–183
 - external users, 141–143
 - groups, 185–186, 188–189
 - Guest, 192
 - home share, 181
 - identity management needs, 276
 - krbtgt, 192
 - modifying attributes, 178–183
 - organizational unit (OU), 15, 79
 - passwords, 176–177
 - policy settings, 289
 - provisioning, 130
 - remote access, 185–186
 - Single Sign-on (SSO), 9, 143
 - Terminal Services, 182–184, 187–188
 - user principal name (UPN), 65, 68–69, 314
 - Users Group, 196
- **V** •
- verifying trusts, 304
 - viewing
 - audit entries, 251–252
 - audit settings, 249
 - default users and groups, 192–196
 - schema, 220–221, 226
 - trusts, 304
 - vision statement, 45

visionary (on implementation planning team), 44
vulnerabilities, 233

• W •

WAN (wide area network), 13
WBADMIN command line tool, 263
Web Enrollment, 163, 165
Web sites
 Confessions of an IT Geek Blog, 283–284
 Directory Services Team Blog, 281
 Exchange Server Team Blog, 281
 Internet Engineering Task Force (IETF), 58
 TechNet Magazine, 280
 Windows IT Pro Magazine, 282
 Windows Server 2008, 279–280
 Windows Server 2008 TechCenter, 280
 Windows Server Team Blog, 282
wide area network (WAN), 13
Wilensky, Marshall, *TCP/IP For Dummies*, 5th Edition, 212
Windows Authorization Access Group, 196
Windows Internet Naming Server (WINS), 70
Windows IT Pro Magazine Web site, 282

Windows Server 2008
 editions, 104–105
 hardware requirements, 103–105
 Hyper-V, 105
 installation, 103–107
 RSS feeds, 283
 TechCenter Web site, 280
 Web site, 279–280
Windows Server Backup tool, 261–263
Windows Server Team Blog, 282
Windows Time Service, 304
WINS (Windows Internet Naming Server), 70
W32™ command line tool, 286, 304

• X •

X.500 directory service standard
 compatibility, 10
 compliance, 10
 defined, 10
 Lightweight Directory Services (LDS), 133
 protocols, 10

• Z •

zones (DNS), 59–62, 70

