

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A

- access restrictions. *See* security
- Account Domains, 138
- account lockout
 - in domain accounts, 21
 - in group policy design, 81
 - problems in, **236–240**, 237–238
- account management, auditing for, 321, 321
- accounts
 - in domain design, **20–21**, 21
 - with GPOs, 269
 - in migration, **143**
 - in OU delegation, 74
 - security for, **282–284**
- acctinfo.dll file, **233**, 234, 237, 238
- Active Directory Application Mode (ADAM), 13, **210–211**, 211–212
 - for domain functional level, 29, 30
 - for FSMO roles, 247, 248
- ADAM (Active Directory Application Mode), 13, **210–211**, 211–212
- ADDT (Active Directory Domains and Trusts)
 - for domain functional level, 29
 - for FSMO roles, 247, 248
- ADLB (Active Directory Load Balancing) tool, 202
- ADMIGRATION.MSI file, 139
- administration boundaries in forest design, **10**
- administrative control, OU design for, **67–73**, 69–72
- administrative groups for Exchange design, **105**
- administrative methods for security, **322–323**
- administrative requirements in OU structure, **94–96**
- AdminSDHolder account changes, auditing, 320
- ADMT (Active Directory Migration Tool)
 - interface, **138–140**, 139
 - in migration, 148
 - in native mode, **34**
 - prerequisites, **140–141**
 - for reconstruction, 156
 - scripting, **143–144**
 - for SIDs, 137
- Adprep utility, 152
- ADSI (Active Directory Services Interface) Edit
 - for Directory Service partitions, **181**, 181–182
 - for display names, 105–107, 106–107
 - for domain functional level, 30, 31
 - for ForestPrep, 101
 - naming contexts in, 7, 7
 - for removing
 - computer accounts, **190**, 190
 - FRS members, **190–191**
 - trustDomain objects, **191**
- Active Directory Installation Wizard, **126–130**, 126–130
- Active Directory-integrated zones, 41, 297
- Active Directory Load Balancing (ADLB) tool, 202
- Active Directory Migration Tool. *See* ADMT (Active Directory Migration Tool)
- Active Directory Schema
 - for ForestPrep, 101
 - for FSMO roles, 249, 249
- Active Directory Services Interface. *See* ADSI (Active Directory Services Interface) Edit
- Active Directory Sites and Services, 191
- Active Directory Sizer, **113–115**, 114–115
- Active Directory Users and Computers (ADUC)

- ADUC (Active Directory Users and Computers)
 - for domain functional level, 29, 30
 - for FSMO roles, 247, 248
 - Advanced tab for FRS, 224, 224
 - Alert Dialog, 222, 223
 - Alert History tab, 221, 222
 - All Inbound Traffic filter, 285
 - Allow Automatic Administrative Logon setting, 281
 - Allow Floppy Copy And Access To All Drives And Folders setting, 281
 - Allow Server Operators To Schedule Tasks setting, 279
 - Allow System To Be Shut Down Without Having To Log On setting, 281
 - Allow Undock Without Having To Log On setting, 279
 - Allowed To Format And Eject Removable Media setting, 279
 - alockout.dll tool, 237
 - Alockout.txt file, 237
 - Aloinfo.exe tool, 237
 - American National Standards Institute (ANSI), 6
 - ANSI (American National Standards Institute), 6
 - answer files, 124–125
 - appinit.reg file, 237
 - application event log, 267
 - application partitions, 7, 210–211, 211–212
 - applications
 - in migration, 155, 161
 - site design for, 56, 57
 - ASR (Automated System Recovery), 174–176, 175–176
 - Asr.sif file, 175, 176
 - Asrnp.sif file, 175, 176
 - asynchronous processing for GPOs, 265, 269
 - attack vectors, 302
 - attacks, 302
 - logon, 240
 - remote access, 276
 - Domain Controller Security Options Policy for, 278–281, 278
 - policy settings for, 276–277, 276
 - user rights assignments for, 277–278
 - attributes
 - for deleted objects, 174
 - in Exchange design, 106–107
 - Audit The Access Of Global System Objects setting, 279
 - Audit The Use Of Backup And Restore Privilege setting, 279
 - auditing
 - domain controllers, 314–320, 315
 - for logon failures, 229–233, 230, 233
 - for remote access attacks, 276–277, 276, 279
 - authentication, 322
 - in domain accounts, 21
 - in domain controller placement, 111
 - in forest design, 9, 9
 - Kerberos logging, 234
 - in multiple domain design, 23–24
 - two-person, 323
 - authoritative restores, 172–173
 - authoritative zone transfers (AXFRs), 48
 - authorization in multiple domain design, 24
 - Automated System Recovery (ASR), 174–176, 175–176
 - automatic processes
 - deployment setup, 124–125
 - display name generation, 105–107
 - domain controller promotion, 134–135
 - update configuration, 308–310, 309
 - Automatic Site Coverage, 56
 - autonomous control in forest design, 11, 12
 - AvoidPdcOnWan value, 241
 - AXFRs (authoritative zone transfers), 48
- ## B
- backup and disaster recovery, 167
 - best practices for, 176–177
 - domain controller backups, 168–169, 169
 - reactive vs. proactive, 167–168
 - restoration in, 170–174, 171–172

Backup Domain Controllers (BDCs), 64, 117
 emulating, 150–151
 in migrating from Windows NT 4, 146
 Backup utility, 168–170, 169, 174
 Bart's Network Boot Disk creator, 123
 baselines in security, 322
 BDCs (Backup Domain Controllers), 64, 117
 emulating, 150–151
 in migrating from Windows NT 4, 146
 binary images in deployment, 125
 BIND (Berkley Internet Name Domain) servers, 47
 Block Inheritance option, 90
 blocking in group policy design, 90
 boundaries
 in domain design, 20–21, 21
 in forest design, 6–8, 7, 10
 bridgehead servers, 52
 bridges, site link, 60–62, 60
 British Standards Institute (BSI), 6
 bulletins, security, 301–303

C

cache poisoning, 295–296
 cached credentials, 323, 324
 caching, universal group membership, 61–62, 113, 235
 CD setup, 125
 Change Control policies, 16–17
 change propagation in DNS design, 48–49
 Check Replication Topology option, 200
 /checkacl switch in GPOTool, 259
 child domains in deployment, 127, 127
 CIFS/SMB filter, 284
 Clarence Washington Script Repository, 326
 Clear Virtual Memory Pagefile setting, 281
 client-side extensions (CSEs) for GPOs, 261–262, 265
 clients in NetWare migration, 160
 cloned images in deployment, 125
 ClonePrinciple utility, 156
 Code Red attacks, 302

column filters for FRS, 224
 command-line utilities for FSMO roles, 249–251
 /commit parameter in ADLB, 203
 committing database transactions, 183–184, 183
 common Global Catalogs, 8
 compacting database, 184–186, 185–186
 Component Status in Group Policy Results, 262
 computer accounts, removing, 190, 190
 Computer Migration Wizard, 139
 Computers container, 92
 conditional forwarders, DNS, 38, 206, 207
 configuration
 automatic updates, 308–310, 309
 diagnostic logging, 179–181, 180
 in replication, 7
 user rights assignments, 277–278
 Configuration Directory Partitions, 316–318
 connected sites, 58
 connections in domain migration, 137–138
 controller.inf files, 277
 corporate standards in group policy design, 84–85,
 89, 89
 costs of site link connections, 59
 countermeasures, 302
 credentials
 cached, 323, 324
 in deployment, 126, 127
 for domain controllers, 134, 134
 criteria
 in domain design, 20–22, 21
 forest design, 4–5
 critical updates, 303
 Cross Site Boundaries option, 202
 CSEs (client-side extensions) for GPOs, 261–262, 265

D

data migration, NetWare, 161
 databases, 179
 attacks on, 295

- best practices for, **192–193**
- compacting, **184–186**, *185–186*
- diagnostic logging for, **179–181**, *180*
- integrity checking, **184**
- maintaining security accounts, **191–192**
- in migration, **140**
- moving, **186–187**
- moving log files, **187**
- placement of, **128**, *128*, **313–320**, *315*
- populating, **131**
- removing orphaned objects, **187–191**, *190*
- space for, **314**
- transactions to, **183–184**, *183*
- troubleshooting and repairing, **182–183**
- DC Comms filter, **285**
- /dc switch in GPOTool, **258**
- DCBP (Default Controller Baseline Policy), **277**
- DCDiag utility
 - for FSMO roles, **251**
 - for migration, **202**
- dcpfix.exe utility, **92**
- [DCInstall] section, **135**
- dcpromo utility, **126–130**, *126–130*, **135**
- DDNS, secure, **295**, *296*
- Debug Logging tab, **214**, *215*
- Default Controller Baseline Policy (DCBP), **277**
- Default Domain Controller Policy, **277**
- Default Domain Policy setting, **21**, *21*, **85**, *91–92*
- default services, security for, **285–287**
- DEFAULTIPSITELINK link, **58**
- defining domain names, **121–122**
- delegating control, **9**, **73–76**
- Delegation of Control Wizard, **74**
- delegation records, **206**, *208*
- Delegation tab, **260**, *260*
- denial of service (DoS) attacks, **289**
- Denied List for GPOs, **264**
- deployment, **121**
 - automatic setup for, **124–125**
 - defining domain names, **121–122**
 - domain controllers in
 - first, **126–130**, *126–131*
 - promoting, **134–135**
 - replica, **131–134**, *133–134*
 - forest root domain identification in, **122–123**
 - manual setup for, **123–124**
 - for patches, **304–306**, **308–311**, *308–309*
- Details tab, **221**, *222*
- Devices settings, **279**
- Devx.com site, **326**
- DFS (Distributed File System), **52**, *217*
- diagnostic logging, **179–181**, *180*
- diagnostic tools for DNS, **212–214**, *213–215*
- Digitally Encrypt Or Sign Secure Channel Data (Always)
 - setting, **279**
- directories, morphed, **218–219**
- directory service access, auditing, **277**
- Directory Service partitions, viewing, **181**, *181–182*
- Directory Services Restore Mode (DSRM), **130**, *130*, **170–171**, *184–185*
- Disable Machine Account Password Changes setting, **279**
- Disable Transitive Replication option, **202**
- disabled GPOs, **264**
- disabling
 - 8.3 auto-name generation, **282**
 - recursion, **293–294**, *294*
- disaster recovery. *See* backup and disaster recovery
- Disconnect Clients When Logon Hours Expire setting, **280**
- disconnected terminal server sessions, **236**
- display name generation, **105–107**
- Distribute Software Updates Wizard Installer, **306**
- Distributed File System (DFS), **52**, *217*
- DNS (Domain Name System), **205**
 - Active Directory Application Mode for, **210–211**, *211–212*
 - best practices for, **215–216**
 - in deployment, **129**, *129*
 - designing, **37–38**

- best practices for, 49
 - change propagation in, 48–49
 - current DNS infrastructure in, 46
 - feature support in, 47–48
 - internal and external namespaces in, 45–46
 - resolution in, 38–39, 39–40
 - zone types in, 40–45, 43–44
 - diagnostic tools for, 212–214, 213–215
 - in forest design, 13
 - in installation security, 282
 - in multiple domain design, 22, 23
 - name standards for, 121–122
 - in replication, 196–198, 197–198
 - resolution methods in, 205–208, 207–208
 - root domain SRV records in, 208–210, 209
- DNS records, removing, 191
- DNS Server filter, 284
- DNS snap-in, 188, 191
- DNSScmd command, 211, 212
- DNSLint command, 196–198, 197–198, 213
- Do Not Allow Storage Of Credentials Or.NET
Passports For Network Authentication setting, 280
- Do Not Display Last User Name setting, 280
- Do Not Require Ctrl+Alt+Del setting, 280
- Domain Controller Security Options Policy,
278–281, 278
- domain controllers, 109
 - auditing, 314–320, 315
 - backups, 168–169, 169
 - credentials for, 134, 134
 - in deployment
 - first, 126–130, 126–131
 - promoting, 134–135
 - replica, 131–134, 133–134
 - IPSec filters for, 284–285
 - in multiple domain design, 26–28
 - operations masters in, 63–65, 116–118
 - orphaned metadata removal, 188–191, 190
 - overrun control, 149–151
 - placement of, 111–112, 118
 - Global Catalogs, 112–113
 - Master Operations, 116–118
 - promotions, automating, 134–135
 - in remote access attacks, 279
 - removing, 191
 - in site topology, 52
 - sizing, 113–115, 114–115, 118
 - specifications for, 110–111
 - in zone replication, 42

domain local groups, 32

Domain Member settings, 279–280

domain migration and consolidation, 137
 - account status in, 143
 - ADMT scripting in, 143–144
 - BDC emulation in, 150–151
 - best practices for, 157
 - connections in, 137–138
 - domain controller overrun in, 149–151
 - domain preparation in, 154–155, 154–155
 - forest preparation in, 152–153, 153
 - options in, 138–140, 139
 - order in, 142
 - passwords in, 144–145
 - preparing for, 140–144
 - profiles in, 142
 - resource domains in, 148, 149
 - rollback plans in, 141–142
 - strategies in, 146–148, 147
 - unique accounts in, 143
 - upgrades vs. reconstruction in, 156
 - utilities for, 156–157
 - from Windows 2000, 151–155, 153–155
 - from Windows NT 4, 145–146

Domain Name System. *See* DNS (Domain Name System)

Domain Naming Masters, 63, 116, 244

Domain Password Policy dialog, 237, 237

/domain switch in GPOTool, 258

/DomainPrep switch, 99, 103–105, 104, 152, 154–155, 154–155

- domains
 - controllers. *See* domain controllers
 - designing, 19
 - best practices for, 34–35
 - criteria in, 20–22, 21
 - multiple domains in. *See* multiple domain design
 - tree requirements in, 21–22
 - for Exchange design, 103–105, 104
 - functional levels in, 13, 28–34, 29–31
 - migration and consolidation. *See* domain migration and consolidation
 - names, 121–122, 127, 127
 - partitions, auditing, 318–319
 - trusts between, 9, 24–25, 25–26
 - in zone replication, 42
 - DoS (denial of service) attacks, 289
 - drive mappings with account lockout problems, 236
 - dsadd quota command, 291, 292
 - dsastat.exe utility, 198–199, 199
 - DsHeuristics attribute auditing, 318
 - dsmod quota command, 291, 292
 - dsquery quota command, 291, 293
 - dsquery server command, 250–251
 - DSRM (Directory Services Restore Mode), 130, 130, 170–171
 - dsutil command, 314
 - dumpfsmos.cmd utility, 251
 - DumpGPOInfo.wsf script, 270
 - dynamic updates, 290
- E**
- edb*.log file, 313
 - 8.3 auto-name generation, 282
 - Emergency Repair Disk (ERD), 174
 - empty GPOs, 264
 - empty roots, 123
 - emulators
 - BDCs, 150–151
 - neutralizing, 151
 - PDCs, 65, 239, 246–247
 - in multiple-domain forests, 64–65, 117–118
 - netlogon.log on, 239
 - EnableKerbLog.vbs script, 238
 - End User License Agreement (EULA), 124
 - enterprise clients, DCBP files for, 277
 - environment logging, 266–268, 267
 - ERD (Emergency Repair Disk), 174
 - ERD Commander utility, 171
 - Estimate Logon Rates option, 114, 114
 - EULA (End User License Agreement), 124
 - Event IDs, 230–232
 - event log files
 - in deployment, 128, 128
 - moving, 187
 - size, 313
 - Event Viewer
 - for account management, 321, 321
 - for FRS, 226
 - logs in, 180
 - EventCombMT tool, 238
 - events
 - in FRS, 226, 226
 - logon, 276–277
 - in security logs, 230
 - Exchange design, 99
 - administrative groups for, 105
 - best practices for, 107–108
 - display name generation in, 105–107
 - domain preparation for, 103–105, 104
 - extended attributes in, 106–107
 - forest preparation for, 100–103, 101–104
 - Exchange Directory Migration Wizard, 140
 - ExDeploy program, 101, 101
 - executive sponsorship, 4
 - Experts Exchange site, 326
 - extended attributes in Exchange design, 106–107
 - external namespaces, 45–46
 - extranet applications, 11, 17

F

FAZAM tool, 256, 261

FDDeploy logging, 268

feature packs, 303

file replication service. *See* FRS (file replication service)

File Replication Service Event Log, 226, 226

filters

for domain controllers, 284–285

for FRS, 224

for GPOs, 87, 87, 90, 262, 264, 269

FindDisabledGPOs.wsf script, 270

FindDuplicateNamedGPOs.wsf script, 270

FindGPOsBySecurityGroup.wsf script, 270

FindGPOsWithNoSecurityFiltering.wsf script, 270

FindOrphanGPOsInSYSVOL.wsf script, 270

FindUnlinkedGPOs.wsf script, 270

firewalls, 61

first domain controllers in deployment, 126–130, 126–131

Flexible Single Master Operations. *See* FSMO (Flexible Single Master Operations) roles

folder redirection, 268

forest root domains, identifying, 122–123

/ForestPrep switch, 99–102, 102, 152–153

forests

designing, 3–4

best practices for, 15–18

common Global Catalogs in, 8

criteria in, 4–5

extranet applications in, 17

functionality modes in, 13–15, 14

Kerberos and trusts in, 9, 9

multiple, 10–13, 12

political and administration boundaries, 10

schema in, 5–6

security boundaries in, 6–8, 7

simplicity in, 15–16

standard scenarios, 17–18

in Exchange design, 100–103, 101–104

functionality levels, 13–15, 14

in migration, 42, 152–153, 153

multiple-domain, operations masters in, 63–65, 116–118

formatting drives, 281

forwarders, DNS, 38, 40, 206, 207

FRS (file replication service), 58, 217

best practices for, 227

FRSDiag for, 220, 221

journal wrap in, 218

MOM for, 225

morphed directories in, 218–219

overview, 217

parallel version vector joins in, 219

problem resolution in, 226, 226

removing members, 190–191

staging areas in, 219

Ultrasound for, 220–225, 221–225

FRSDiag tool, 220, 221

FSMO (Flexible Single Master Operations) roles, 243

best practices for, 253–254

current role holders, 247–251, 248–250

Domain Naming Masters, 244

importance of, 243

Infrastructure Masters, 244–245

PDC emulators, 246–247

placement, 62–65, 116–118

Relative Identifier Masters, 245–246

in restores, 172

Schema Masters, 244

seizing, 252–253

tools for, 247–251, 248–250

transferring, 251–252

function, OU design based on, 70, 70

functionality modes in forest design, 13–15, 14

G

GALs (Global Address Lists), 8

GCs. *See* Global Catalogs (GCs)

General section in Group Policy Results, 261

- Global Address Lists (GALs), 8
 - Global Catalog Server filter, 284
 - Global Catalog servers
 - for Master Operations roles, 116
 - in replication, 132, 133
 - Global Catalogs (GCs)
 - in domain controllers, 112–113
 - in forest design, 8
 - hard drive space for, 110
 - in multiple domain design, 27–28
 - in native mode logons, 235
 - placement, 61–62
 - globally unique IDs (GUIDs)
 - for bridgehead servers, 52
 - in registration, 196–197
 - GPMC (Group Policy Management Console), 93
 - Group Policy Modeling, 80, 80, 260
 - Group Policy Results, 260–263, 261–263
 - for troubleshooting, 259–260, 259–260
 - working with, 78–80, 79–80
 - /gpo switch in GPOTool, 258
 - GPOs (group policy objects). *See* group policy and GPOs
 - GPOTool, 258–259
 - GPResult tool, 256–257, 258, 260–263, 261–263
 - Group Account Migration Wizard, 139
 - Group Mapping and Merging Wizard, 140
 - group nesting in native mode, 33
 - group policy and GPOs, 77–80, 255
 - application issues, 264–266
 - auditing, 229, 230, 319–320
 - best practices for, 270
 - considerations in, 268–269
 - design for, 80–84
 - diagnostics tool for, 259
 - environment logging for, 266–268, 267
 - GPOTool for, 258–259
 - Group Policy Management Console for. *See* Group Policy Management Console (GPMC)
 - inheritance in, 88–90, 88–89, 91, 265
 - interoperability issues in, 86–87, 87
 - linking, 91–92
 - minimizing, 86
 - objectives in, 80–84
 - scripts with, 269–270
 - user requirements in, 84–86
 - Group Policy Creator Owners group, 95
 - Group Policy Management Console (GPMC), 93
 - Group Policy Modeling, 80, 80, 260
 - Group Policy Results, 256–257, 258, 260–263, 261–263
 - for troubleshooting, 259–260, 259–260
 - working with, 78–80, 79–80
 - Group Policy Modeling, 80, 80, 260
 - Group Policy Modeling Wizard, 93
 - Group Policy Results, 256–257, 258, 260–263, 261–263
 - Group Policy Results Wizard, 261, 264–265
 - Group Policy template, 173
 - GroupWise, moving from, 162
 - GUIDs (globally unique IDs)
 - for bridgehead servers, 52
 - in registration, 196–197
 - [GUIRunOnce] section, 135
- ## H
- hardware sizing and placement, 109
 - best practices for, 118
 - placement of, 111–112, 118
 - Global Catalogs, 112–113
 - Master Operations, 116–118
 - sizing, 113–115, 114–115, 118
 - specifications for, 110–111
 - headless forest roots, 123
 - Health tab, 221
 - high security, DCBP files for, 277
 - hotfixes, 303
- ## I
- IANA (Internet Assigned Numbers Authority), 6

IAS (Internet Authentication Service) servers, 240

ICMP filter, 285

identity confusion, 45–46

IgnoreGCFailures keys, 235

IIS in installation security, 282

important security bulletins, 303

inaccessible GPOs, 264

Incident Log, 224–225, 225

incremental zone transfers (IXFRs), 48

inetorgpersonfix.ldf file, 155

Infrastructure Masters, 64, 117, 244–245

inheritance

in group policy and GPOs, 88–90, 88–89, 91, 265

in OU delegation, 75–76

installation, security during, 281–282

integrated service packs, 303

integrating patches, 306–311

integrity, database, 184

Interactive Logon settings, 280

interforest trusts, 24–25, 25–26

internal namespaces, 45–46

Internet Assigned Numbers Authority (IANA), 6

Internet Authentication Service (IAS) servers, 240

Internet protocol security (IPSec)

for domain controllers, 284–285

in group policy design, 82

for security, 295

interoperability issues

in domain functional levels, 28

in group policy design, 86–87, 87

Intersite Topology Generator (ISTG), 52, 200

IP protocol for replication, 58

IPSec (Internet protocol security)

for domain controllers, 284–285

in group policy design, 82

for security, 295

isolation in forest design, 11, 12

ISTG (Intersite Topology Generator), 52, 200

IXFRs (incremental zone transfers), 48

J

job functions and requirements in group policy design, 85–86

journal wrap, 218

just-in-time training, 163

K

KCC (Knowledge Consistency Checker), 52, 200

Kerberos authentication

in domain accounts, 21

in forest design, 9, 9

in multiple domain design, 24

Kerberos filter, 284

Kerberos logging, 234

KIXtart utility, 162

Klez-E attacks, 302

Knowledge Consistency Checker (KCC), 52, 200

L

large organizations, replication in, 202–203

LDAP changes, auditing, 318

LDAP Client Signing Requirements setting, 281

LDAP Server filter, 284–285

LDP.exe tool, 30

legacy clients, DCBP files for, 277

levels

domain functionality, 13, 28–34, 29–31

forest functionality, 13–15, 14

logging, 266

lifetimes, tombstone, 132, 174

linking group policies, 91–92

links, site, 58–62, 60

ListallGPOs.wsf script, 270

local-only names, 122

local profiles in migration, 142

Local Security Authority (LSA), 283

location, OU design based on, 68, 69, 71–72, 71–72

locking down transfers, 298–299, 298

- lockout
 - in domain accounts, 21
 - in group policy design, 81
 - problems in, **236–240**, 237–238
 - LockoutStatus.exe utility, 237, 237
 - locks, 275
 - log files and logging
 - in deployment, 128, 128
 - diagnostic, 179–181, 180
 - for Group Policy, **266–268**, 267
 - Kerberos, 234
 - moving, 187
 - size, 313
 - /log parameter in ADLB, 203
 - logon Event IDs, **230–232**
 - Logon Type entry, 232–233
 - logons, **229**
 - account lockout problems, **236–240**, 237–238
 - attacks in, **240**
 - auditing, **229–233**, 230, 233, 276–277
 - best practices for, **241**
 - and domain controller placement, 111
 - estimating, 114, 114
 - Kerberos logging, **234**
 - in multiple designs, 23
 - native mode, **235–236**
 - remote access issues, **240**
 - secondary, **322**
 - WAN communication in, **240–241**
 - loopbacks, GPO, **90**, 265, 269
 - low security bulletins, 303
 - LSA (Local Security Authority), 283
- M**
- mail migration, **161–162**
 - Manage Auditing And Security Log right, 105
 - management, auditing, 276, 321, 321
 - manual deployment setup, **123–124**
 - mapped devices in NetWare migration, **162**
 - Master Operations. *See* FSMO (Flexible Single Master Operations) roles
 - Master User Domains (MUDs), **146–148**, 147
 - Maximum Machine Account Password Age setting, 279
 - MBSA (Microsoft Baseline Security Analyzer) utility, 302, 304–305, 305
 - memory for domain controllers, 110
 - metadata, orphaned, **187–189**, 190
 - Microsoft Baseline Security Analyzer (MBSA) utility, 302, 304–305, 305
 - Microsoft Directory Synchronization Services (MSDSS), 160–161, 163
 - Microsoft Identity Integration Server 2003 (MIIS), 8, 13
 - Microsoft Network Client settings, 280
 - Microsoft Network Server settings, 280
 - Microsoft Operations Manager (MOM) tool, **225**
 - migration
 - domain. *See* domain migration and consolidation
 - NetWare. *See* NetWare migration
 - MIIS (Microsoft Identity Integration Server 2003), 8, 13
 - minimizing GPOs, **86**
 - moderate security bulletins, 303
 - MOM (Microsoft Operations Manager) tool, **225**
 - monitoring
 - reactive vs. proactive, **167–168**
 - traffic, **290**
 - Monitoring Client filter, 284
 - morphed directories, **218–219**
 - most restrictive/most inclusive nesting strategy, 33
 - MoveTree utility, 156–157
 - moving
 - accounts, 269
 - database, **186–187**
 - log files, 187
 - _msdcs subdomain, 209, 209
 - MSDN Windows Script, 326
 - msDS-Behavior-Version attribute, 30

MSDSS (Microsoft Directory Synchronization Services), 160–161, 163
MSN Scripting Group, 326
MUDs (Master User Domains), 146–148, 147
multiple domain design, 22
 authentication options in, 23
 DNS requirements in, 22, 23
 domain controller placement in, 26–28
 domain functional levels in, 28–34, 29–31
 interforest trusts in, 24–25, 25–26
 operations masters in, 63–65, 116–118
multiple forests, 10–13, 12

N

Name Servers tab, 298

names

 8.3 auto-name generation, 282
 domain, 121–122, 127, 127
 Exchange display name generation, 105–107
 in NetWare migration, 163
 in replication, 7
 site links, 58
 zones, 37, 44–45

namespaces

 in DNS design, 45–46
 in security, 290

native mode, 31–34

 ADMT in, 34
 domain local groups in, 32
 group nesting in, 33
 logon failures, 235–236
 NETLOGON synchronization in, 34
 SIDHistory in, 34
 universal groups in, 32–33

NDS (NetWare Directory Services), 3

nesting groups in native mode, 33

NetBIOS names in deployment, 128, 128

NetBIOS Server filter, 284

NetDom utility, 156, 250

NetLogon

 logging, 238–239
 synchronization, 34

NETLOGON folder, 217

netlogon.log file, 239

NetWare Directory Services (NDS), 3

NetWare migration, 159

 application compatibility in, 161
 best practices for, 164
 data migration, 161
 mail migration, 161–162
 mapped devices in, 162
 MSDSS for, 163
 preparing for, 159–160
 testing in, 162
 training in, 162–163

Network Access settings, 280

network infrastructure

 in forest design, 13
 with GPOs, 268
 identifying design, 53, 54

network maps, 53–55, 54

Network Security settings, 281

networks, replication across, 131–132

neutralizing emulators, 151

Nimda attacks, 302

NLParse tool, 238–240

nltest command, 238

No Auto-Restart for Scheduled Automatic Updates

 Installations setting, 309

non-Active Directory-integrated zones, 297–298

normal restores, 172

nslookup command, 212

NTBugtraq mailing list, 302

ntds.dit file, 313

NTDSUTIL utility

 for application partitions, 210
 for authoritative restores, 173
 best practices for, 192–193
 for committing transactions to database, 183–184, 183

- for compacting database, 184–186, 185–186
- for database integrity, 184
- for DSRM password, 170–171
- for FSMO roles
 - seizing, 253
 - transfer, 251–252
- for maintaining security accounts, 191–192
- for moving
 - databases, 186–187
 - log files, 187
- for removing orphaned objects, 187–191, 190
- for troubleshooting, 182–183
- NTFS Change Journal, 218
- NTFS file system, 281
- NTP Server filter, 285
- Number of Previous Logons To Cache (In Case Domain Controller Is Not Available) setting, 280

O

- Object Identifiers (OIDs), 5–6
- objectives in group policy, 80–84
- objects, 5
 - auditing access to, 277
 - orphaned, 187–191, 190
 - visibility of, 76–77, 77–78
- OIDs (Object Identifiers), 5–6
- one-way synchronization, 163
- operating systems, 3–4
 - best practices for, 281–282
 - for GPOs, 266
- Optional Subsystems setting, 281
- order in migration, 142
- organization
 - forest design based on, 17
 - OU design based on, 68–72, 69, 71–72
- orphaned objects, 187–191, 190
- OU (organization unit) design and structure, 67, 92–93
 - for administrative control, 67–73, 69–72
 - administrative requirements in, 94–96
 - best practices for, 96
 - choosing, 73

- for delegating control, 73–76
- for group policy. *See* group policy and GPOs in NetWare migration, 160
- object visibility in, 76–77, 77–78
- Outlook and Outlook Web Access, 236
- overrun control, 149–151
- owners in OU delegation, 74–75

P

- parallel version vector joins, 219
- parent-child trusts, 24
- parent domains in deployment, 127
- Partition_FQDN command, 211
- partition-level auditing, 317–318
- partitions
 - Directory Service, 181, 181–182
 - in replication, 7
- Password Export Servers (PESs), 145
- passwords
 - acctinfo.dll for, 233, 234
 - in domain accounts, 21
 - DSRM, 170–171
 - in group policy design, 81
 - LSA for, 283
 - in migration, 144–145
 - Syskey for, 283–284
- patches, 301
 - best practices for, 312
 - deployment plans for, 304–306, 308–311, 308–309
 - integrating, 306–311
 - security bulletins and announcements for, 301–302
 - testing, 304
 - third-party solutions, 311
 - updates for, 302–304
- PDCs (Primary Domain Controllers)
 - emulators, 246–247
 - in multiple-domain forests, 64–65, 117–118
 - netlogon.log on, 239
 - in migrating from Windows NT 4, 145–146

- permissions
 - for auditing, **315–316**, 315
 - in deployment, 130, 130
 - DomainPrep switch for, 105
 - in OU delegation, 75–76
 - in OU design, 95–96
 - persistent drive mappings, 236
 - personnel, trustworthy, **322–323**
 - PESs (Password Export Servers), 145
 - physical access
 - to domain controllers, 26–27, 111
 - security for, 275–276
 - policies
 - auditing changes to, 277
 - group. *See* group policy and GPOs
 - for remote access attacks, 276–277, 276
 - Policy events tab, 263
 - political boundaries in forest design, 10
 - populating databases, 131
 - PredefinedRPC Range filter, 285
 - Prevent Users From Installing Printer Drivers setting, 279
 - Primary Domain Controllers (PDCs)
 - emulators, **246–247**
 - in multiple-domain forests, 64–65, 117–118
 - netlogon.log on, 239
 - in migrating from Windows NT 4, 145–146
 - primary restores, 171–172, 171–172
 - primary zones, 40–42
 - priority in group policy design, 90, 91
 - privilege use, auditing, 277
 - proactive management vs. reactive, 167–168
 - process tracking, auditing, 277
 - processors for domain controllers, 110
 - profiles in migration, 142
 - programs, lockout problems with, 236
 - promotion, domain controller, 134–135
 - Prompt User To Change Password Before Expiration setting, 280
 - protar.mdb database, 140
 - protocols for replication, 58
 - pull replication, 200
 - pwdmig.exe utility, 144
- ## Q
- quotas, 291, 292–293
- ## R
- RAM for domain controllers, 110
 - reactive management vs. proactive, 167–168
 - reconstruction vs. upgrades, 156
 - Recovery Console settings, 281
 - recursion, disabling, 293–294, 294
 - redircmp.exe utility, 93
 - redirection for environment logging, 268
 - rediruser.exe utility, 93
 - refresh cycles, GPO, 265–266
 - Refuse Machine Account Password Changes setting, 279
 - registering names, 121–122
 - Registry settings
 - for automatic update client, 310
 - for logging levels, 179–181, 180
 - relative identifier (RID) Masters
 - in multiple-domain forests, 63–64, 117
 - working with, 245–246
 - remote access attacks, 276
 - Domain Controller Security Options Policy for, 278–281, 278
 - policy settings for, 276–277, 276
 - user rights assignments for, 277–278
 - Remote Installation Services (RIS), 83, 125
 - Remote Procedure Calls (RPC), 58
 - removing
 - computer accounts, 190, 190
 - DNS records, 191
 - domain controllers, 191
 - FRS members, 190–191
 - orphaned objects, 187–191, 190
 - trustDomain object, 191

- repadmin utility, **200**
 - replica domain controllers, **131–134**, *133–134*
 - replication
 - best practices for, **203–204**
 - configuration in, **7**
 - DCDiag for, **202**
 - DNS problems in, **196–198**, *197–198*
 - of DNS zones, **41–42**
 - in domain design, **21**, **35**
 - for GPOs, **266**, **268**
 - in large organizations, **202–203**
 - across networks, **131–132**
 - overview, **195–196**
 - repadmin for, **200**
 - ReplMon for, **200–202**, *201*
 - site design for, **56**
 - site links in, **59**, *59*
 - verifying, **198–202**, *199*, *201*
 - ReplMon utility
 - for FSMO roles, **249**, *250*
 - for troubleshooting, **200–202**, *201*
 - Reporting Wizard, **140**
 - Require Domain Controller Authentication To Unlock Workstation setting, **280**
 - Require Smart Card setting, **280**
 - Require Strong (Windows 2000 Or Later) Session Key setting, **280**
 - Reschedule Automatic Updates Scheduled Installations setting, **309**
 - reserve files, **314**
 - Reset Account Lockout Counter After setting, **236**
 - resolution
 - in DNS design, **38–39**, *39–40*
 - methods, **205–208**, *207–208*
 - resource domains, **138**, **148**, *149*
 - resource forests, **17**
 - resources
 - in forest design, **13**
 - in OU delegation, **74**
 - Restore Wizard, **171**, *171*
 - restoring, **170**
 - authoritative restores, **172–173**
 - Automated System Recovery for, **174–176**, *175–176*
 - Directory Services Restore Mode, **170–171**
 - normal restores, **172**
 - primary restores, **171–172**, *171–172*
 - tombstones in, **173–174**
 - Restrict Anonymous Access To Named Pipes And Shares setting, **280**
 - Restrict CD-ROM Access To Locally Logged On User Only setting, **279**
 - Restrict Floppy Access To Locally Logged On User Only setting, **279**
 - restricted-access forests, **17**
 - RID (relative identifier) Master role
 - in multiple-domain forests, **63–64**, **117**
 - working with, **245–246**
 - rights. *See* permissions
 - RIS (Remote Installation Services), **83**, **125**
 - roaming profiles, **142**
 - roaming users, **113**
 - rollback plans in migration, **141–142**
 - root domain SRV record availability, **208–210**, *209*
 - root domains, identifying, **122–123**
 - root zones, **38**, *39*
 - routing, security for, **294**
 - Routing and Remote Access Service (RRAS), **240**
 - row filters for FRS, **224**
 - RPC (Remote Procedure Calls), **58**
 - RPC Server filter, **284**
 - RRAS (Routing and Remote Access Service), **240**
- ## S
- schedules for site links, **59**
 - schema in forest design, **5–6**
 - Schema Management MMC snap-in, **8**
 - Schema Masters
 - in multiple-domain forests, **63**, **116**

- purpose of, 244
- viewing, 249, 249
- schema partitions
 - auditing, 315–316, 315
 - in replication, 7
- scope of zone replication, 41–42
- Script Center site, 325
- Scripting newsgroup, 326
- ScriptLogic utility, 162
- Scriptomatic, 325
- scripts
 - ADMT, 143–144
 - for environment logging, 268
 - with Group Policy, 269–270
 - resources for, 325–326
- secondary logons, 322
- secondary zones, 42, 206
- secure DDNS, 295, 296
- Secure Installation Location, 282
- security, 275, 289
 - Active Directory, 313
 - administrative methods for, 322–323
 - baselines in, 322
 - best practices for, 323–324
 - database file placement, 313–320, 315
 - service account administrators, 321, 321
 - in deployment, 130, 130
 - for DNS, 289
 - access restrictions, 296–298
 - best practices for, 299
 - cache poisoning, 296
 - disabling recursion, 293–294, 294
 - dynamic updates in, 290
 - IPSec, 295
 - locking down transfers, 298–299, 298
 - monitoring for traffic, 290
 - quotas in, 291, 292–293
 - for routing, 294
 - secure DDNS, 295, 296
 - separate namespaces for, 290
 - for domain controllers, 111, 275
 - best practices for, 287–288
 - default services, 285–287
 - during installation, 281–282
 - IPSec filters, 284–285
 - for remote access attacks, 276–281, 276, 278
 - for well-known user accounts, 282–284
 - in domain design, 35
 - for environment logging, 268
 - in extranet applications, 17
 - in forest design, 6–8, 7
 - GPO filtering, 264, 269
 - in group policy design, 81–82
 - patches for. *See* patches
 - security accounts, 191–192
 - security bulletins and announcements, 301–303
 - Security Group Membership When Group Policy Was Applied section, 262
 - security identifiers (SIDs), 34
 - in migration, 137–138, 146
 - RID Masters for, 245
 - security ratings, 303
 - Security Translation Wizard, 140
 - Security Update Inventory Installer, 305–306
 - Security Update Inventory tool, 306
 - Security Update Sync tool, 306
 - seizing FSMO roles, 252–253
 - Send Unencrypted Password To Third-Party SMB
 - Servers setting, 280
 - separate namespaces, 290
 - server rooms, locking, 275
 - servers in NetWare migration, 160
 - Service Account Migration Wizard, 140
 - service accounts
 - administrators for, 321, 321
 - security for, 283
 - Service Level Agreements (SLAs), 82
 - service packs, 282, 303
 - Set Password On Site DC option, 234, 234
 - Settings tab, 262–263, 263

- Setup Manager, **124–125**
- shortcut trusts, **24–25, 26**
- Shut Down System Immediately If Unable To Log
 - Security Events setting, **279**
- Shutdown settings, **281**
- SIDHistory attribute, **137**
 - in migration, **141–142**
 - in native mode, **34**
- SIDs (security identifiers), **34**
 - in migration, **137–138, 146**
 - RID Masters for, **245**
- simplicity in design
 - domain, **34**
 - forest, **15–16**
 - Group Policy, **84**
- single domain forests
 - Master Operations placement in, **116**
 - operations masters in, **63**
- site link bridges, **60–62, 60**
- site link design, **58–60**
- sites
 - in AD design, **55–56, 55, 57**
 - auditing, **317**
 - best practices for, **65–66**
 - in domain controller placement, **27**
 - network infrastructure in, **53, 54**
 - topology, **51–53**
- size
 - domain controllers, **113–115, 114–115, 118**
 - event log files, **313**
- SLAs (Service Level Agreements), **82, 86**
- slow link processing restrictions for GPOs, **266**
- Smart Card Removal Behavior setting, **280**
- SMS (Systems Management Server)
 - for group policy, **83**
 - for patch deployment, **310–311**
- SMTP protocol, **58**
- software installation for group policy, **82–83, 259**
- Software Update Services (SUS) server, **305, 308–311, 308–309**
- Software Updates Installation Agent, **306**
- specifications for domain controllers, **110–111**
- Specify Intranet Update Service Location setting, **309**
- SQL Slammer attacks, **302**
- SRV records
 - in DNS design, **37**
 - high availability, **208–210, 209**
- /stagger parameter in ADLB, **203**
- staging areas in FRS, **219**
- standard forest scenarios, **17–18**
- standard forwarders, **206, 207**
- standard logons, **23**
- standard primary zones, **40**
- standards
 - DNS names, **121–122**
 - in group policy design, **84–85, 89, 89**
- standby domain controllers, FSMO roles on, **252–253**
- Strengthen Default Permissions Of Internal System
 - Objects (E.G. Symbolic Links) setting, **281**
- strong passwords, **81**
- stub zones, **42–44, 43–44, 206**
- subnets, **53**
- Summary tab
 - in FRS, **223, 223**
 - in Group Policy Results, **261–262, 262**
- Support Tools, **156**
- SUS (Software Update Services) server, **305, 308–311, 308–309**
- synchronization
 - in native mode, **34**
 - in NetWare migration, **163**
- Synchronize This Directory Partition option, **202**
- Syskey utility, **283–284**
- sysprep utility, **125**
- system events, auditing, **277**
- System objects settings, **281**
- system profiles, **142**
- System State data
 - backing up, **168–169, 169**
 - in replication, **132, 133**

Systems Management Server (SMS)
 for group policy, 83
 for patch deployment, 310–311
Systems Settings setting, 281
Sysvol folder
 accessing, 217
 group policy templates in, 128, 129, 173

T

task-based delegation, 74
TCO (total cost of ownership), 148
TCP/IP in installation security, 282
temp.edb file, 313
templates, Group Policy, 128, 129, 173
Terminal Services Server filter, 284
testing
 NetWare migration, 162
 patches, 304
third-party patch solutions, 311
threat agents, 302
threats, 302
tombstones, 173–174
 lifetime, 132, 174
 quotas on, 291
Topology Changes tab, 221
total cost of ownership (TCO), 148
traffic, monitoring for, 290
training
 in NetWare migration, 162–163
 in OU design, 94–95, 94
transactions, database, 183–184, 183
transferring FSMO roles, 251–252
transfers, zone, 48–49, 298–299, 298
transitive trusts, 9
tree-root trusts, 24
trees in domain design, 21–22, 35
Trojan.Kaht attacks, 302
Trust Migration Wizard, 140
trustDomain object, removing, 191

trusts
 in forest design, 9, 9
 for GPOs, 268
 in migration, 141
 in multiple domain design, 24–25, 25–26
trustworthy personnel, 322–323
Tweakomatic, 325
two-person authentication, 323
two-way synchronization, 163
two-way trusts, 9, 25

U

Ultrasound tool, 220–225, 221–225
unattend.txt file, 124–125
unique accounts in migration, 143
universal group membership caching, 61–62, 113, 235
universal groups, 32–33
unnecessary services, 285–287
Unsigned Driver Installation Behavior setting, 279
update rollups, 303
Update Sequence Numbers (USNs), 200
updates
 automatic configuration of, 308–310, 309
 dynamic, 290
 for patch management, 302–304
upgrades vs. reconstruction, 156
Use Certificate Rules On Windows Executables For
 Software Restrictions Policies setting, 281
User Account Migration Wizard, 139
User Principle Names (UPNs), 23
userenv.log, 267, 267
UserEnv (User Environment) logging, 266–268, 267
users
 configuring rights assignments, 277–278
 distributing to domain controllers, 115, 115
 in group policy design
 requirements, 84–86
 restrictions, 83–84

training

in NetWare migration, 162–163

in OU design, 94–95, 94

Users container, 92

USNs (Update Sequence Numbers), 200

V

/verbose switch in GPOTool, 259

verifying replication, 198–202, 199, 201

virtual systems, 11, 304

visibility in OU design, 76–77, 77–78

VMWare systems, 11, 304

vulnerabilities, 302

W

WAN links and communication

in AD design, 55

for domain controllers, 111–112

for Global Catalogs, 112–113

in logon failures, 240–241

in replicating across networks, 132

with site link bridges, 62

well-known user accounts, security for, 282–284

WHQL (Windows Hardware Quality Labs) signatures, 304

Windows 2000, migration from, 151–155, 153–155

Windows 2000 Mixed Mode functional level, 28

Windows 2000 Native Mode functional level, 28, 30, 31–34

Windows Hardware Quality Labs (WHQL) signatures, 304

Windows Management Instrumentation (WMI)
for FRS, 221

for GPOs, 87, 87, 262, 264, 269

Windows NT 4, migration from, 145–146

Windows Scripting Newsletter, 326

Windows Server 2003 functional level, 28–29

Windows Server 2003 Interim functional level, 29–30

Windows Update, 307, 307

WMI (Windows Management Instrumentation), 221
for FRS, 221

for GPOs, 87, 87, 262, 264, 269

workstations in NetWare migration, 160

WQL (WMI query language) tests, 264

Z

zone transfers, 48–49, 298–299, 298

zones

access to, 297–298

in DNS resolution, 206

names, 37, 44–45

primary, 40–42

secondary, 42, 206

stub, 42–44, 43–44, 206