

Index

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

Numbers

6to4 tunneling, 69–70

A

access control lists (ACLs), 170
and GPOs, 207

accessibility, and domain
controller location, 23

Active Directory
authentication, 17–18
groups in, 176
replication, with DNS, 77–78

Active Directory domain
structure, 13–18
creation, 17
functional levels, 13–14
regional domain model, 16
single and multiple domains,
14, 15

Active Directory Federation
Services (AD FS), 33, 33–36

Active Directory forest, 5. *See*
also forest structure design

Active Directory-integrated
applications, 154

Active Directory Migration Tool
(ADMT), 97
default screen, 101
instantiating, 99
options, 100–102

Active Directory Rights
Management Services (AD
RMS), 32–33, 297

Active Directory schema, 11. *See*
also schema

Add Role Services wizard,
258–260

Configure Cryptography for
CA page, 259

Select Role Services page, 258

Specify Setup Type page, 259

Add Roles Wizard

for Hyper-V

Create Virtual Networks
page, 361

Installation Progress page,
361

Installation Results page,
362

Select Server Roles page,
360

for Online Responder Service

Installation Progress page,
257

Select Role Services page,
257

Select Server Roles page,
256, 256

address prefix, of IPv6
address, 62

administrative model, 2–3
administrative structure, and
certificate authority
hierarchy, 248–249
administrative template files,
215, 308

ADMT. *See* Active Directory
Migration Tool (ADMT)

ADMX GPO templates, 215

adprep command, 125

adprep /domainprep command,
119

adprep /forestprep command,
119

adprep /rodcprep command, 120

agents, for SCVMM, 371

all-ones subnets, avoiding, 56

AMD-V, for Hyper-V, 352

anycast address, 63

APIPA addressing, 48–49

application layer attacks, 83

application virtualization,
151–156, 348

Active Directory-integrated
applications, 154

anatomy, 152–153

components and software,
154–155

line-of-business applications,
153

process, 152

scaling enterprise with,
156–157

operating system, 157

user support, 156

strategy implementation, 158

applications
updates to, 314
using old, 159

audits, levels of, 188

Authenticated Users group, 208
authentication

Active Directory, 17–18

certificate-based, 80–81

cross-forest, 110–118

forestwide, 112–113, 113

selective, 112–113, 113

trust policy for, AD FS and,
34

authentication protocols,
password-based policy,
79–80

authoritative restores, 288

authoritative transfers (AXFRs),
77

authority, delegating, 182

Authority Information Access
(AIA), monitoring, 250

autoenrollment, 264

Automatic Tunneling Pseudo-
Interface, 70

autonomous forest model, 11

autonomous mode, for WSUS
downstream server, 316

autonomy

in forest design, 8

in OU design, 174

AXFRs (authoritative transfers),
77

B

back-to-back firewalls, 85

backup domain controller
(BDC), 23, 30

Backup Once Wizard

Backup progress, 296

Select backup configuration,
294

Specify advanced option, 295

Specify destination type, 294

Specify remote folder, 295

backup, Windows Server 2008,
285–286

- base certificate revocation lists, 252
 - bastion host, 84
 - BIOS, enabling hardware virtualization, 359
 - BitLocker (Windows), 31, 287
 - Block Policy Inheritance, 175, 185
 - in Group Policy, 205–206
 - bootable WinRE disk, 289
 - branch offices, Server Core installation for, 121
 - bridged connection, for virtual machine, 357
 - broadcast addresses, 58, 63
 - built-in local groups, 177–178
 - business continuity, 274. *See also* RAID (redundant array of independent disks)
 - Active Directory Rights Management Services (AD RMS), 297
 - Distributed File System (DFS), 279–281
 - Encrypting File System, 286–287
 - exam essentials, 298
 - failover clustering, 281–282
 - network load balancing, 283–284
 - quorums, 283
 - recovering Active Directory Domains Services, 287–288
 - with Server Core, 296
 - Volume Shadow Copy, 289–296
 - Previous Versions tab, 290
 - Windows BitLocker, 31, 287
 - Windows Recovery Environment, 288–289
 - Windows Server backup tools, 285–286
 - business function-based OU hierarchy, 172
-
- C**
- centralized-decentralized model, 3, 4
 - centralized design model, 3, 4
 - certificate authority (CA), 252
 - hierarchy, 245–247
 - modeling structure, 248–249
 - managing to communicate with online responder, 260–261
 - certificate-based authentication, 80–81
 - Certificate Request Wizard, 263
 - certificate revocation lists (CRLs), 252
 - certificate templates, 252, 261
 - certificates
 - for SSL encryption, 143, 144
 - X.509 digital certificate, 249–250
 - certificates MMC, 263
 - certification policy, 245
 - certification practice statement (CPS), 245
 - certreq.exe, 263
 - certutil.exe, 250–251
 - Challenge Handshake Authentication Protocol (CHAP), 80
 - chglogon.exe, 150
 - child OUs, inheritance, 185
 - claims-aware agent, 36
 - Class C address, default subnet mask for, 52
 - class levels of IP addresses, 49–50
 - client access licenses (TS CALs), 137
 - client-side deployment of updates, 325
 - Client Side Extension (CSE), 220
 - clients
 - automatic search for new update server, 324
 - controlling behavior for RemoteApp programs, 149
 - enterprise or specialized environments, 309
 - managing external, 262
 - for OCSP, 255
 - records in WINS database, 73
 - CNAME records, GlobalNames zones use of, 74
 - collaborative forest model, 11
 - combination OU hierarchy, 173, 173
 - command-line enrollment, 263
 - command prompt, for recovery, 289
 - comments for GPOs, 218–219
 - communication, initial process in Teredo, 71
 - compliance, 335–336
 - compliance auditing, 187
 - computer accounts, migration, 106–109
 - computer group, for WSUS, 325
 - Computer Migration Wizard, 102, 107–109
 - Domain Selection, 107
 - Organizational Unit Selection, 108
 - Translated Objects, 109
 - computer, restarting, 123
 - cone flag, 71
 - connectivity, maintaining, 123–124
 - consolidation, 348
 - Control Panel, Windows Update icon, 330
 - CRL distribution (CDP) extensions, monitoring, 250
 - CRLs (certificate revocation lists), 252
 - cross-forest authentication, 110–118
 - Cryptography Next Generation, 261, 262
 - Custom GPO permission, 212
-
- D**
- DACL (discretionary access control list), 169
 - data autonomy, 8
 - data isolation, 8
 - database server
 - for Active Directory Rights Management Services, 32
 - for SCVMM, 372
 - dcgpofix.exe tool, 211
 - decentralized design model, 4–5
 - default domain policy, 211–212
 - avoiding GPOs with WSUS specifications, 225
 - delegation
 - of Group Policy administration, 212–213
 - planning, 182–185
 - Delegation of Control Wizard Tasks to Delegate, 184
 - Users or Groups, 183
 - delta certificate revocation lists, 252
 - demilitarized zone (DMZ), 83
 - denial-of-service attacks, 83
 - design, 2
 - design models, 2–5
 - centralized, 3, 4
 - decentralized, 4–5

- exam essentials, 37
- hybrid, 5
- desktop virtualization, 348
- device installation, Group Policy
 - for controlling by users, 228–229
- DFS. *See* Distributed File System (DFS)
- DHCP (Dynamic Host Control Protocol), 49
 - host NAT for virtualized pool, 356
 - server placement, 86
 - version 6, 66
- discretionary access control list (DACL), 169
- disk space. *See* hard drives
- Distributed File System (DFS), 279–281
 - components, 279
 - failover, 280
 - redundant namespace servers, 281
 - referral ordering, 280
 - replication, 280
 - target priority, 281
- distribution groups, 176
- “DLL hell”, 153
- DLLs (dynamic link libraries), 153
- DMZ (demilitarized zone), 83
- DNS (Domain Name Service)
 - Active Directory replication with, 77–78
 - servers, requirements and placements, 78–79
- documentation, on updates
 - before downloading, 334
- domain controllers
 - avoiding GPOs with WSUS specifications, 225
 - disk space requirements, 24
 - memory requirements, 24
 - placing, 23–24
 - processor requirements, 24
 - read-only (RODCs), 30–31, 31
 - recovering, 287
- domain level, for licensing, 138
- domain local groups, 177
 - planning, 180
- Domain Name Service (DNS). *See* DNS (Domain Name Service)
- domain naming master,
 - location, 26
- domain policy, default, 211–212

- domain Properties dialog box,
 - Trusts tab, 117
- domain trusts, 19–20, 110
- domains
 - consolidating, real world scenario, 99–100
 - joining Server Core to, 122–123
 - structure design, 13–18
 - creation, 17
 - functional levels, 13–14
 - regional domain model, 16, 16
 - single and multiple domains, 14, 15
- downloading
 - Hyper-V update, 359
 - SUSE Linux Enterprise edition, 367
- downstream server in WSUS, 315–316
- driver store, 228
- drivers
 - signing, 229
 - updates to, 314
- dual IP stacking, 66–67
- dual layer addressing, 67
- Dynamic Host Control Protocol (DHCP), 49
 - host NAT for virtualized pool, 356
 - server placement, 86
 - version 6, 66
- dynamic IP addressing, 49
 - IPv6, 64–66
- dynamic-link libraries (DLLs), 153

E

- EAP-TLS (Extensible Authentication Protocol-Transport Level Security), 80
- Easy Print, 147–148
- Edit Settings GPO permission, 212
- EFS (Encrypting File System), 286–287
- EKU (extended key usage), 80
- email notifications from WSUS server, 326
- Enable Connections Through the TS Gateway Group Policy setting, 149
- enabled group policies, 148

- Encrypting File System (EFS), 286–287
- encryption
 - BitLocker, 31
 - certificates for SSL, 143, 144
- enforced group policies, 149
- enrollment agents, 264
- enrollment strategies, for PKI, 262–263
- enterprise administrator, 5
 - job of, 151
- enterprise certificate authorities, 253
- enterprise client environments, 309
- enterprise, designing for large-scale, 181
- environments
 - legacy, public key infrastructure in, 245
 - technical limitations, 347
- Ethernet port, sharing, 356
- ethics, 175
- EUI-64, 64–65, 65
- Event ID 28: “TS Licensing Service is unable to report status...”, 140
- Event ID 37: “TS Licensing Cannot Start...”, 140
- Event ID 100, 144
- Event ID 1001, 145
- Event ID 1005, 145, 146
- Event ID 1041, 151
- events, codes, 151
- Exchange 5.5 Mailbox
 - Translation Wizard, 102
- experimentation, to determine server location, 137
- extended key usage (EKU), 80
- Extensible Authentication Protocol-Transport Level Security (EAP-TLS), 80
- external clients, managing, 262
- external namespaces, 74–76
 - design, 75
- external trusts, 19, 19, 110
- external virtual networks, 358

F

- failover clustering, 281–282
 - quorums for, 283
- failover, in DFS, 280
- FAT32, Volume Shadow Copy and, 291
- fault tolerance, requirements of TS licensing, 140

Federated Web SSO design, 34, 35
 with forest trust design, 35
 federation scenarios, 34
 Federation Services proxy, 36
 federation trust, 34, 35
 file share witness, 283
 firewalls, 83
 classes, 84
 network location awareness and change in, 219
 options, 84–85
 firmware, updates to, 314
 floppy drives, Hyper-V limits, 353
 folders, in DFS structure, 279
 forest collaboration, 6
 forest level, for licensing, 138
 forest structure design, 5–12
 autonomy vs. isolation, 8
 design elements, 7
 functional levels, 6–7
 models, 8–10
 organizational, 9, 9
 resource-based, 10
 restricted-access, 10, 10
 schema, 11–12
 modification, 12
 single-forest vs. multiple-forest design, 11–12
 forest trusts, 9, 18–19, 110
 creating, 115–118
 establishing business, 114
 forest upgrades, planning, 118–125
 forest and domain preparation, 119
 preparing for read-only domain controller, 119–120
 Server Core install preparation, 121
 forestwide authentication, 112–113, 113
 four-tier CA structure, 247, 248

G

geography, and network design, 21–22, 22
 global accounts, planning, 180
 global catalog, 25
 global catalog server, 25
 global groups, 177
 GlobalNames zones, 77
 for transition from WINS to DNS, 73–74

gpupdate /force command, 225
 Group Account Migration Wizard, 101–102
 Group Policy, 168, 308
 applying, 203–206
 inheritance, 204, 204–205
 order, 203
 configuring automatic updates, 224–225
 controlling user installation of devices, 228–229
 default domain policy, 211–212
 delegating administration, 212–213
 deploying in single large domain, 213–214
 exam essentials, 234
 loopback processing, 206
 new Windows Server 2008 features, 214–224
 administrative template files, 215
 comments for GPOs, 218–219
 network location awareness, 219
 preferences, 219–224
 starter GPOs, 215–216
 in OU design, 174
 planning, 210–211
 design for infrastructure, 211
 restrictions and objectives, 210
 restricting group memberships with, 225–228
 scope, 202–203
 security categories, 213
 security filtering, 206–209
 on Terminal Services, options and changes, 147–149
 Group Policy links, delegating control of administration, 184
 Group Policy Management
 default domain controllers policy setting, 207
 Group Policy Management Editor
 Computer Configuration
 Control Panel Settings, 221, 221–222
 Windows Settings, 220, 220–221
 User Configuration
 Control Panel Settings, 223, 223
 Windows Settings, 222, 222

Group Policy Modeling Tool, 231–233, 232
 Group Policy objects (GPOs), 202
 creating for WSUS use, 322
 permissions table, 212
 searching, 229–231
 security filtering on, 209
 Group Policy standards, 5
 group SID, 169
 groups
 in Active Directory, 176
 delegating control of administration, 184
 planning for, 180–182
 scope, 176–180
 altering, 178, 179

H

hard drives
 domain controller requirements, 24
 Hyper-V limits, 353
 hardware firewall, 84
 hardware RAID, 275
 hardware statistics, 313
 hardware virtualization-based rootkit, 352
 honey pot, 83
 host bits, calculating, 52
 host NAT, for virtualized DHCP pool, 356
 Host only connection, for virtual machine, 357
 host portion
 of IPv6 address, 62
 of subnet mask, 52
 hosts
 tunneling between, 68–69
 tunneling between router and, 69, 69
 HTTPS (Hypertext Transfer Protocol Secure) protocol, 265
 over RDP, for Terminal Services Gateway server access, 142
 hybrid administration model, 5
 hybrid design model, 5
 Hyper-V, 349, 351–354
 failover and recovery with, 356
 hardware requirements, 351–352
 installing, 359–366
 preparation, 359
 limits, 352–353

setting up, 363–366
 through Remote Desktop, and
 enabled mouse, 368
 Windows Vista x64
 management, 369
 Hyper-V Manager, 355, 363,
 363
 Hypertext Transfer Protocol
 Secure (HTTPS) protocol,
 265
 over RDP, for Terminal
 Services Gateway server
 access, 142
 hypervisor, 351

I

IAS (Internet Authentication
 Server), 81
 ICANN (Internet Corporation
 for Assigned Names and
 Numbers), 63
 incoming one-way trusts, 111
 incremental zone transfers
 (IXFRs), 77
 inetOrgPerson accounts,
 delegating control of
 administration, 185
 .inf files, 308
 infrastructure master, 26
*Infrastructure Planning and
 Design Guide for Microsoft
 SoftGrid*, 157
 inheritance, 185–186, 186
 of Group Policy, 204,
 204–205
 inherited design, 22, 23
 initial client configuration, with
 Teredo, 71
 installation CD, for Windows
 Recovery Environment, 289
 installing
 devices by users, Group Policy
 for controlling, 228–229
 Hyper-V, 359–366
 Online Responder service,
 256–258
 operating system, on virtual
 machine, 366–368
 read-only domain controllers
 (RODCs), 120
 SUSE Linux Enterprise
 edition, 368
 updates, 332
 Windows Server Backup, 292,
 292–296, 293
 instantiating ADMT, 99
 Intel VT, for Hyper-V, 352
 interface ID, of IPv6 address, 62
 interforest trusts, 113
 intermediate certificate authority
 role, 253
 internal namespaces, 74–76
 design, 76
 internal virtual networks, 357
 Internet Authentication Server
 (IAS), 81
 Internet Corporation for
 Assigned Names and
 Numbers (ICANN), 63
 Internet Explorer, for Microsoft
 Update, 333
 Internet Protocol Security
 (IPsec), 80–81
 Internet Protocol version 4
 (IPv4)
 addressing and subnetting,
 51–61
 addressing given topology,
 53, 53–56
 available hosts and subnets,
 51–53
 transition to IPv6, 66–71
 Internet Protocol version 6
 (IPv6), 49
 address ranges, 50–51
 address types, 63
 addressing, 61–66
 shorthand notation, 61–62
 anatomy, 62–63
 IPv4 transition to, 66–71
 static and dynamic
 addressing, 64–66
 Internet service provider (ISP),
 63
 Internet Small Computer
 Systems Interface (iSCSI),
 368–369
 Intra-Site Automatic Tunnel
 Addressing Protocol
 (ISATAP), 70
 intraforest trusts, 113
 intrusion attacks, 83
 IP spoofing, 83
 ipconfig command, 66, 219
 IPsec (Internet Protocol
 Security), 80–81
 IPv6 over IPv4 packet, 67, 68

ISATAP (Intra-Site Automatic
 Tunnel Addressing
 Protocol), 70
 iSCSI (Internet Small Computer
 Systems Interface),
 368–369
 isolation, in forest design, 8
 ISP (Internet service provider), 63
 issuing certificate authorities, 253
 IXFRs (incremental zone
 transfers), 77

J

jump drive, change in size, 228

K

Kerberos, for transitive trust, 19
 knowledge consistency checker
 (KCC), 27

L

Layer 2 Tunneling Protocol
 (L2TP), 82
 legacy environment, public key
 infrastructure in, 245
 legal requirements, for forests, 7
 liability issues, 97
 library server, for SCVMM, 372
 limited-functionality
 environment, 309
 line-of-business applications,
 153
 Linux distributions
 Hyper-V support, 354
 and Windows, 372
 load balancing, Terminal
 Services across sessions,
 145
 locally installed virtualized
 application, 152
 location-based OU hierarchy,
 172
 logical Internet protocol
 address, 65
 logical unit numbers (LUNs), 369
 loopback processing, in Group
 Policy, 206

M

- Mac OS X, running Windows XP through virtualized desktop, 348, 349
 - manual assignment, in IPv6, 65
 - mapping, 143
 - membership of groups, delegating control of administration, 184
 - memory
 - domain controller requirements, 24
 - Hyper-V limits, 353
 - Merge mode, in loopback processing, 206
 - Microsoft Baseline Security Analyzer tool, 310, 310
 - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), 79
 - Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), 80
 - Microsoft Download Center, 368
 - Microsoft MCITP enterprise administrator exam, design logic and decision process, 21
 - Microsoft Report Viewer, 316
 - Microsoft SoftGrid, 151. *See also* SoftGrid
 - Microsoft Solution Accelerator for Windows Server 2008 security, 309
 - Microsoft Solution Accelerator Guides for Windows Server 2008*, 157
 - Microsoft System Center Configuration Manager, 155
 - Microsoft System Virtual Application Server (SVAS), 154
 - Microsoft Update, 333
 - Microsoft Virtual PC 2004 and 2007, 155, 157, 159
 - migration, 96–97
 - caution with, 97–98
 - of computer accounts, 106–109
 - of objects, 98–99
 - of user accounts, 102–106
 - migration log, for computer accounts, 109
 - mirroring (RAID 1), 276
 - “mixed RAID” mode, 277
 - monitoring Terminal Services Licensing, 140
 - mouse, Hyper-V through Remote Desktop and, 368
 - MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 79
 - MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2), 80
 - .msi file extension, 153
 - multicast addresses, 63
 - multimaster replication engine, 280
 - multiple-domain architecture, 14, 15
 - multiple-forest schema, vs. single-forest design, 11–12
 - multitasking, vs. virtualization, 349–350
 - multitiered OU infrastructure, 205
-
- ## N
- name resolution, in WINS, 72–73
 - namespaces
 - in DFS, 279
 - redundant servers, 281
 - internal and external, 74–76
 - NAT (Network Address Translation), 50, 70
 - and external namespace, 75
 - NAT-T (Network Address Translator Traversal), 70–71
 - National Security Agency (NSA) standards for network security, 335
 - nesting OUs, 170
 - .NET Framework, 121
 - netsh interface ipv4 show
 - interfaces command, 122
 - netsh interface isatap set router
 - command, 70
 - network access policies, 82–83
 - network adapters
 - listing of, 122
 - multiple, in virtual networks, 358
 - Network Address Translation (NAT), 50, 70
 - and external namespace, 75
 - Network Address Translator Traversal (NAT-T), 70–71
 - network addressing
 - defining ranges, 56
 - IPv4, 51–61
 - IPv6, 61–66
 - anatomy, 62–63
 - shorthand notation, 61–62
 - ranges, 49–51
 - for IPv4 addresses, 49–50
 - for IPv6 addresses, 50–51
 - readdressing, real world scenario, 57–58
 - techniques, 48–49
 - variable-length subnet masking (VLSM), 58–61, 59
 - Network Device Enrollment Service, 264
 - network interface cards. *See* network adapters
 - network load balancing, 283–284
 - network location awareness, 219
 - network policy server (NPS), 81–83
 - placement, 85
 - network reconnaissance, 83
 - network structure
 - creation, 2
 - physical requirements and topology, 21–26
 - domain controller placement, 23–24
 - restrictions, 21–22
 - networks
 - Hyper-V limits, 353
 - legacy, and Windows Server 2008, 71–74
 - perimeter, 83–85
 - planning for access, 79–86
 - server placement, 85–86
 - setups with virtual machines, 356–357
 - virtual, 357–358
 - New Conditional Forwarder dialog box, 115–116, 116
 - New Starter GPO dialog box, 216, 216
 - New Virtual Machine Wizard
 - Assign Memory page, 364
 - Completing the New Virtual Machine Wizard, 366
 - Configure Networking page, 365
 - Connect Virtual Hard Disk, 365

Specify Name and Location
page, 364
nltest tool, 115
No Override option for Group
Policy inheritance, 205–206
nonauthoritative restores, 288
nontransitive trusts, 112
NPS (network policy server),
81–83
placement, 85
ntbackup.exe, 285
Ntdis.dit, 287
NTFS, Volume Shadow Copy
support for, 291

O

object-based delegation,
182–183
object type-based hierarchy,
172, 173
objects
consolidating, 98–99
migration of, 98–99
security descriptors, 169
obstructions, and network
design, 22
OCSP (Online Certificate Status
Protocol), 254–255
components, 255
octet of concern, 55
Olsen, Gary, 97
one-way trusts, 111, 111
Online Certificate Status
Protocol (OCSP), 254–255
components, 255
online responder, 255
managing CA to communicate
with, 260–261
Online Responder service, 254
installing, 256–258
operating system
installing on virtual machine,
366–368
storing files separately, 288
supported guest with
Hyper-V, 353–354
updates to, 313
virtualizing, 350
operational requirements, for
forests, 7
operations master, roles, 25–26
organizational forest model, 9, 9
organizational requirements, for
forests, 7
organizational units (OU),
170–173
creating reasonable structure,
210
design requirements, 174–175
hierarchy, 170–173, 172
business function-based,
172
combination, 173, 173
location-based, 172
object type-based, 172, 173
for migrated accounts, 105
OU administrator, 176
OU owner, 176
outgoing one-way trusts, 111
owner
of object, 169
of organizational unit, 176

P

packet sniffers, 83
parity bits, 276, 276
Password Authentication
Protocol (PAP), 80
password-based policy
authentication protocols,
79–80
Password Migration Wizard,
102
passwords, delegating control of
administration, 184
patch Tuesday, 334
PEAP (Protected Extensible
Authentication Protocol),
80
per-device licensing, 138
per-session default printers, 148
per-user licensing, 138
perimeter networks, 83–85
possible intrusion attacks, 83
permissions, of objects, 169
personal firewall, 84
physical MAC address, 65
ping command, 123, 219
PKI. *See* public key
infrastructure (PKI)
PKI Health tool, 250
pkiview.msc command, 250
planning, 2
delegation, 182–185
for existing forest upgrades,
118–125
forest and domain
preparation, 119
preparing for read-only
domain controller,
119–120
Server Core install
preparation, 121
Group Policy, 210–211
design for infrastructure,
211
restrictions and objectives,
210
for groups, 180–182
for network access, 79–86
for reduction, 123–124
schema modification, 12
Point-to-Point Protocol (PPP), 67
policy, 168
policy certificate authority
role, 253
ports
443 for Terminal Services
Gateway server, 143
AD RMS exception
requirements, 32
PowerShell, 121
PPTP (Point-to-Point Tunneling
Protocol), 82
precedence, in Group Policy, 204
preferences
for GPOs, 219–224
vs. policy, 219
prefix portion, of IPv6 address,
50, 62
presentation virtualization, 348
primary domain controller
(PDC), 26, 30
primary zones, 76
printer scope redirection, 148
printing, with Terminal Services-
based applications, 147
private virtual networks, 358
processors
domain controller
requirements, 24
Hyper-V limits, 353
productivity, loss from
equipment failures, 311
Protected Extensible
Authentication Protocol
(PEAP), 80
public key infrastructure (PKI),
244
components, 251–252
managing external clients,
262
modeling after administrative
structure, 248–249
reasons for, 251
push/pull process, for WINS
replication, 73

Q

quorums, 283

R

RADIUS (Remote Authentication Dial-In User Service), 81

RAID (redundant array of independent disks), 274–278

- configurations, 275–278
- RAID 0 (striping), 275
- RAID 1 (mirroring), 276
- RAID 5, 276–277
- RAID 10, 277–278

decisions, 278

hardware RAID, 275

for Hyper-V, 351

software RAID, 274–275

RDC (Remote Differential Compression) protocol, 280

RDP. *See* Remote Desktop Protocol (RDP)

Read GPO permission, 212

read-only DNS, 31

read-only domain controllers (RODCs), 30–31, 31

- installing, 120
- preparing for, 119–120

realm trusts, 20, 21, 110

recovery from backup, 296

reduction, planning for, 123–124

redundant namespace servers, in DFS, 281

referral ordering, in DFS, 280

regional domain model, 16, 16

Regional Internet Registry (RIR), 63

relative identifier master (RID master), 26

reliability, and domain controller location, 23

remote access

- policies, 79
- to virtual applications, 152

Remote Authentication Dial-In User Service (RADIUS), 81

Remote Desktop, Hyper-V through, and enabled mouse, 368

Remote Desktop Protocol (RDP) connections, 151

for Terminal Services, 146

for Terminal Services Gateway server access, 142

Remote Differential Compression (RDC) protocol, 280

Remote Procedure Call (RPC) over IP, 27

Remote Server Administration Tools (Vista), 220, 369

RemoteApp programs, controlling client behavior for, 149

Replace mode, in loopback processing, 206

replica mode, for WSUS

- downstream server, 316

replication, 27

- Active Directory, with DNS, 77–78
- in DFS, 280
- WINS, 73

Reporting Wizard, 102

reports, from WSUS, 326–327, 327

research, on updates before downloading, 334

resource-based forest model, 10

resource record (RR), RAM for, 78

restricted-access forest model, 10, 10

restricted enrollment agents, 264

restricted groups, 225

- creating, 226–228

Resultant Set of Policy, delegating control of administration, 184

Retry Task Wizard, 102

revocation providers, for OCSP, 255

RIR (Regional Internet Registry), 63

Roboclient (Robocli.exe), 137

Roboserver (Robosrv.exe), 137

rollback, after update failure, 335

roll-out, of schema modification, 12

root certificate authority, 252–253

- configuring, 258–260

rootkit, 352

router firewall, 84

routers, 52

- tunneling between, 68, 68
- tunneling between host and, 69, 69

S

SACL (system access control list), 169

scalability, network load balancing for, 284

scavenging, 73

schedule, for updates, 334

schema

- for forests, 11–12
- for regional domain model, 16

schema master, location, 25

schema policy, 11

scope

- levels for licensing, 138
- of replication pertaining to DNS, 77–78

scope of management (SOM), 202

SCSI (Small Computer Systems Interface), 369

SCW. *See* Security Configuration Wizard (SCW)

searching Group Policy objects (GPOs), 229–231

secondary zones, 76

Secure Sockets Tunneling Protocol (SSTP), 265

security

- design features, 30–31
- and domain controller location, 23
- in enterprise-level infrastructure, 244–245
- certificate authority hierarchy, 245–247
- certificate authority roles, 252–253
- certificate-monitoring tools, 250–251
- certificate templates, 261
- certification policy, 245
- Cryptography Next Generation, 262
- design factors, 249
- enrollment agents, 264
- enrollment strategies, 262–263
- enrollment types, 263–264
- managing external clients, 262
- modeling structure, 248–249
- Network Device Enrollment Service, 264
- Online Certificate Status Protocol (OCSP), 254–255

- security policy, 244
 - X.509 digital certificate, 249–250
 - internal and external naming
 - addresses for, 75
 - Server Core and, 296
 - for Terminal Services Gateway, 143, 144
 - virtual private networks (VPN) and, 265
 - security baseline, 308–309
 - Security Configuration Wizard (SCW), 187–188, 188
 - security filtering, in Group Policy, 206–209
 - security groups, 176
 - Security Translation Wizard, 102
 - selective authentication, 112–113, 113
 - server availability, 311–312, 312
 - server consolidation, 350, 350–354
 - Server Core, 296
 - installation, 122–123
 - preparing for, 121
 - joining to domain, 122–123
 - static IP addressing for, 122
 - and virtualization, 370
 - server downtime, 313
 - server farm, unbalanced, 284
 - server firewall, 84
 - server node, in cluster, 282
 - server uptime, 312
 - server virtualization, 349
 - servers
 - dedicated for update deployment, 314
 - for global catalog, 25
 - limited functionality portion, 309
 - placing, 85–86
 - roles, 30
 - for SCVMM, 371
 - Service Account Migration Wizard, 102
 - service autonomy, 8
 - service availability, 313
 - service isolation, 8
 - Set the TS Gateway Server Address Group Policy setting, 149
 - Set TS Gateway Authentication Method Group Policy setting, 149
 - shadow copies, 289
 - shared storage, in clustering, 282
 - shortcut trusts, 19–20, 20, 110, 113
 - shutdown /r /t 0 command, 123
 - Simple Certificate Enrollment Protocol, 264
 - Simple Mail Transfer Protocol (SMTP), 27
 - simplicity, single domain and, 15
 - simulating updates, 335
 - single-domain architecture, 14, 15
 - single-forest schema, vs. multiple-forest design, 11–12
 - single sign-on (SSO), 33
 - single-tier CA structure, 246
 - site-link bridges, 29, 29
 - site-link cost, 27
 - site-link schedule, 28–29
 - site links, 27–29
 - sites, 27
 - smart card certificates, enrollment agent for, 264
 - SMTP (Simple Mail Transfer Protocol), 27
 - snapshots, of virtual machine, 355
 - SoftGrid, 151, 153, 154, 155–156, 348
 - infrastructure planning and design, 157
 - SoftGrid administrators, 156
 - SoftGrid browsers, 155
 - SoftGrid Client, SystemGuard, 154
 - SoftGrid Management Web Services, 155
 - SoftGrid Sequencer, 155
 - SoftGrid users, 156
 - software firewall, 84
 - software RAID, 274–275
 - SOM (scope of management), 202
 - specialized client environment, 309
 - SQL Server
 - for SCCM 2007, 328
 - for SCVMM, 371
 - SSO (single sign-on), 33
 - SSTP (Secure Sockets Tunneling Protocol), 265
 - stand-alone certificate authorities, 253
 - starter GPOs, 215–216
 - stateful DHCP, 66
 - stateless configuration, 66
 - stateless DHCP, 66
 - static IP addressing, 49
 - IPv6, 64–66
 - for Server Core server, 122
 - static libraries, 152
 - striping (RAID 0), 275
 - stub zones, 77
 - subdivided mask, 55, 55
 - subdomain, internal namespace as, 75
 - subnet, 27
 - subnet bits portion, of network portion of subnet mask, 53
 - subnet mask, 49
 - determining, 52
 - determining sufficient space in, 54
 - subnet zero subnets, avoiding, 56
 - subnetting, 51
 - for IPv4 addresses, 51–61
 - subnetworks, determining number of, 53
 - SUSE Linux Enterprise edition
 - downloading, 367
 - installing, 368
 - SVAS (System Virtual Application Server), 154
 - synchronized schedule, for WSUS, 326
 - system access control list (SACL), 169
 - System Center Configuration Manager 2007, 328
 - System Center Essentials 2007 (SCE 2007), 327–328
 - System Center Virtual Machine Manager 2007 (SCVMM 2007), 370–372
 - system health model, 311–313
 - hardware statistics, 313
 - server availability, 311–312, 312
 - server downtime, 313
 - server uptime, 312
 - service availability, 313
 - System Virtual Application Server (SVAS), 154
 - SystemGuard, 154
 - SYSVOL directory, 287
-
- T**
- target priority, in DFS, 281
 - targets, in DFS structure, 279
 - task-based delegation, 183
 - Teredo, 70–71
 - Terminal Server, 136
 - Terminal Services
 - client access licenses (TS CALs), 137
 - Easy Print, 147–148
 - Group Policy, options and changes, 147–149

- maintenance and error recovery, 149–151
 - for presentation
 - virtualization, 348
 - roles, 136
 - server load, 136–137
 - Terminal Server drain mode
 - feature, 150, 150
 - Terminal Services connection
 - authorization policies (TS CAPs), 142
 - Terminal Services Gateway, 136, 141–144
 - events, 144
 - Group Policy, 148–149
 - protocols and requirements, 142–143
 - security, 143, 144
 - server placement, 143
 - Terminal Services Licensing, 136, 137–140
 - determining scheme, 141
 - events, 140
 - monitoring, 140
 - process, 139
 - scope, 138
 - server placement, 139–140
 - Terminal Services resources
 - authorization policy (TS RAP), 142
 - Terminal Services Session Broker (TS BB), 136, 144–146
 - events, 145–146
 - load balancing, 145
 - requirements, 145
 - Terminal Services Web Access, 136, 146, 147
 - testing
 - internal virtual networks for, 357
 - schema modification, 12
 - updates before deploying, 335
 - three-homed firewall, 85
 - tier model, for certificate authority hierarchy, 246–247
 - topology, IPv4 addressing for, 53, 53–56
 - transitivity of trusts, 112
 - trust policy, for authentication, AD FS and, 34
 - trusts
 - domain, 19–20
 - forest, 9, 12, 18–19
 - one-way, 111, 111
 - scopes, 113–114
 - tools, 115
 - transitivity, 112
 - two-way, 111, 112
 - types, 110
 - tunneling, 67–70
 - between devices, 68–70
 - two-tier CA structure, 246, 247
 - two-way transitive forest trust, 18
 - two-way trusts, 111, 112
-
- ## U
- Unassigned Computers group, 325
 - universal groups, 177
 - changing, 182
 - creating, with multiple domain membership, 179–180
 - planning, 181
 - Unix users, relationship with Windows server, 20, 21
 - update process, 308. *See also* Windows Software Updates Services (WSUS)
 - compliance, 335–336
 - deployment in medium-sized environment, 329
 - exam essentials, 337
 - Microsoft Update, 333
 - real-world practices, 334–335
 - upstream in WSUS, 315
 - User Account Migration Wizard, 101, 103–106
 - Domain Selection, 103
 - Object Property Exclusion, 106
 - Organizational Unit Selection, 105
 - Password Options, 105
 - User Selection Option, 104
 - user accounts
 - delegating control of administration, 182, 184
 - migrating, 102–106
 - user installation of devices, Group Policy for controlling, 228–229
 - users, informing of major updates, 334
-
- ## V
- variable-length subnet masking (VLSM), 58–61, 59
 - vs. standard subnetting, 60
 - verification, 250
 - virtual COM ports, Hyper-V limits, 353
 - virtual machine, snapshots of, 355
 - virtual machines
 - installing operating system, 366–368
 - network setups, 356–357
 - virtual networks, 357–358
 - multiple network interface cards with, 358
 - virtual optical drives, Hyper-V limits, 353
 - virtual private network (VPN), 81
 - network location awareness and change in, 219
 - security and, 265
 - server placement, 85
 - Virtual Server 2005 Release 2, 349, 372
 - virtualization, 346–347. *See also* application virtualization
 - exam essentials, 373
 - machine components, 354–356
 - vs. multitasking, 349–350
 - and Server Core, 370
 - types, 348–350
 - Virtualization Management Console (VMC), 355
 - viruses, 83
 - visibility, in OU design, 174–175
 - VLSM (variable-length subnet masking), 58–61, 59
 - vs. standard subnetting, 60
 - Volume Shadow Copy, 289–296
 - enabling, 291–292
 - Previous Versions tab, 290
 - VPN (virtual private network). *See* virtual private network (VPN)
-
- ## W
- WAN links
 - for DNS server, 78
 - for forests, 124, 124
 - Wbadmin command line tool, 285–286
 - web-based virtualization, 152
 - web enrollment, 263
 - web farm, 284
 - Web SSO design, 34
 - Windows 2000 domain controller, 125

- Windows 2000, Hyper-V support, 354
 - Windows 2000 Native functional level
 - for domains, 13
 - for forests, 6
 - Windows, and Linux, 372
 - Windows BitLocker, 31, 287
 - Windows Complete PC Restore, 289
 - Windows Deployment Services (WDS), 289
 - Windows Internet Name Service (WINS), 72–73
 - Windows Management Instrumentation (WMI) filters, 209
 - Windows Memory Diagnostic tool, 289
 - Windows NT 4, primary domain controller for, 26
 - Windows Recovery Environment, 288–289
 - Windows Server 2000, average available RAM, 123
 - Windows Server 2003 functional level
 - for domains, 13
 - for forests, 6
 - Windows Server 2003, Hyper-V support, 353–354
 - Windows Server 2008
 - adding in live environment, 124–125
 - administration and delegation features, 32–36
 - automatic update risks, 329
 - average available RAM, 123
 - backup, 285–286
 - clustering with, 282
 - GPMC search tool, 229, 230
 - Group Policy new features, 214–224
 - administrative template files, 215
 - comments for GPOs, 218–219
 - network location awareness, 219
 - preferences, 219–224
 - starter GPOs, 215–216
 - legacy networking and, 71–74
 - migration costs, 97
 - naming conventions, 74–79
 - internal and external namespaces, 74–76
 - NSA security guide for, 336
 - public key infrastructure (PKI), 245
 - security design features, 30–31
 - upgrading forest to, 125
 - Windows Server 2008 functional level
 - for domains, 14
 - for forests, 6
 - Windows Server Backup, installing and using, 292, 292–296, 293
 - Windows Server Core. *See* Server Core
 - Windows Server Deployment Kit, 137
 - Windows server, Unix users' relationship with, 20, 21
 - Windows Server Update Services
 - 3.0 SP1 Setup Wizard, 317–318
 - Windows Server Update Services Configuration Wizard, 318–320
 - Windows Software Updates Services (WSUS), 225
 - anatomy, 315–316
 - groups, 325
 - installing, 316–321
 - options, 326–327
 - planning and implementing, 313–325
 - reports, 326–327, 327
 - server deployment, 315
 - setting up, 321–324
 - update hierarchy and administration decisions, 316
 - Windows token-based agent, 36
 - Windows Update, 329–332
 - history, 331
 - home screen, 330, 331
 - Windows Vista
 - Hyper-V support, 354
 - Remote Server Administration Tools, 220
 - upgrading, and old applications, 159
 - Windows Vista x64 Hyper-V management, 369
 - Windows XP, Hyper-V support, 354
 - WINS (Windows Internet Name Service), 72–73
 - WINS servers, support estimate, 79
 - witness disks, 283
 - wizards, in ADMT, 101–102
 - WMI (Windows Management Instrumentation) filters, 209
 - workflow, update timing to minimize interruption, 334–335
 - workgroup level, for licensing, 138
 - WSUS. *See* Windows Software Updates Services (WSUS)
 - WSUS Administrators group, 314
 - WSUS Management User Services screen, 325
 - WSUS Reporters group, 314
 - WSUS Server Configuration Wizard, 326
 - wuauctl.exe /detect-now command, 324
-
- ## X
- X.509 digital certificate, 249–250
 - XML format, for ADMX files, 215
-
- ## Z
- zone transfers, 77
 - zones, 76–77