Index

Symbol
> (redirection) operator, 65

A
About files, PowerShell, 55–56
activation, 10–11
  KMS (Key Management Service), 10–11
  MAK (Multiple Activation Key), 10
  OEM (Original Equipment Manufacturer) licensing, 10
Active Directory Users and Computers, 292–293
AD (Active Directory)
  auditing, 360–362
  authentication, containers, 280–281
  domain controllers
    auditing, 360–362
    counts, 354
    CPUs, 357–358
    forest root, 354
    Global Catalog servers, 354
    logging, 360–362
    memory, 358–359
    operating system, 354–355
    operating system components, 362–363
    placement, 354
    Remote Desktop, 363
    Remote Management, 363
    sizing, 357–360
    storage, 359–360
    UAC (User Account Control), 363
    Windows Defender, 363
    Windows Firewall, 363
ESAE (Enhanced Security Administrative Environment), 318–319
logging, 360–362
OU (organization unit), creating, 351–353
PAM (Privileged Access Management), 319–321
AD CS (Active Directory Certificate Services), 385
CA (Certification Authority)
  certificate templates, 406–417
  database, 386
  enterprise subordinate installation, 400–406
  placement, 393
  configuration, 402
  results, 402
  key attestation enrollment, 386
  keys, TPM, 386
  network devices, 386
  new features, 385–386
  over-the-air enrollment, 386
  PFX files, 386–387
PKI (public key infrastructure)
  certificate policies, 390
  certificates, 387–388
  CSP (Certificate Practice Statement), 390
documentation, 389–390
  email services and, 392
  encryption and, 392
  environment management, 392
  four-tier hierarchy, 392
  HTTPS and, 387
  intermediate CA, 388
  issuing CA, 388
  LDAPs and, 387
  policies and procedures, 388
  primary components, 387–388
  root CA, 387–388, 394–399
  servers, 393
  single-tier hierarchy, 391
templates, 388
  three-tier hierarchy, 391
tiers, 391–392
two-tier hierarchy, 391, 393
two-tier hierarchy implementation, 393–406
  web services and, 392
PowerShell, 386
role services
  Certificate Authority, 388
  Certificate Authority Web Enrollment, 389
  Certificate Enrollment Policy Web Service, 388
  Certificate Enrollment Web Service, 389
  NDES (Network Device Enrollment Service), 389
  Online Responder, 389
  servers, PKI (public key infrastructure), 393
site awareness, 386
Version 4 templates, 386
Windows Server 2012, 386–387
Windows Server 2012 R2, 386
AD DS (Active Directory Domain Services), 180
Active Directory Recycle Bin, 370
computer management, 363
  schema classes, 364
computer objects, 364
domains
  child domains, 343
  forest root domain, 343
  objects, 342
  parent domains, 343
forests, 342
domains, 342, 343
multiple, 343–344
security boundaries, 342
FSMO (Flexible Single Master Operation)
  roles, 350
  domain naming master, 351
  infrastructure master, 351
  PDC emulator, 351
  RID master, 351
  schema master, 351
GPO (Group Policy Object), 374
  links, PowerShell and, 380
  reports, 378–379
  searching for, 377–378
  settings, PowerShell and, 379–380
Group Policy, 373, 374
  enforcement, 376
  inheritance, 375–376
  linking, 375
  tasks, 376–377
  troubleshooting, 380–382
groups, 370
  adding members, 373
  creating, 372–373
  distribution, 371
  scopes, 371
  security, 371
  token sizes and, 371–372
IPv4 configuration, 181
LSA (Local Security Authority), 371–372
  objects, 342
PAM (Privileged Access Management), 339
  JEA, 341
  JIT, 341
  MIM, 341
replication
  configuration, 349
  domain, 349
  high-level, 349
KCC (Knowledge Consistency Checker), 348
PowerShell, 350
RPC over IP, 349
  schema, 348
  SMTP, 349
sites, 345–347
  link design, 347–348
  trusts, 344–345
user management, 366–368
Windows Server 2003 at End of Life, 339
Windows Server 2012
  Active Directory Recycle Bin, 340
  DAC (Dynamic Access Control), 340
  Fine-Grained Password Policies, 340
  virtualization, 340
Windows Server 2012 R2
  Conditional Access, 340
  Multifactor Authentication, 340
  Workplace Join, 340
  Work Folders and, 252
AD FS (Active Directory Federation Services)
  account partner organization, 425
AD DS domain, 430
  application access
    external client, 452–454
    internal client testing, 445–446
  authentication, 423
  certificates, 432
  claims, 425
  claims provider, 425
  deployment, 433–454
  external client, application access, 452–454
  federation servers, 430
  gMSA (group-managed service account), 432–433
  identity federation, 424
  infrastructure, 430
  internal client, application access, 445–446
  internal DNS name resolution, 439–440
  DNS Manager host, 441
  DNS Manager zone, 440
  overview, 426–428
  planning and design, 429
  component placement, 429–431
  relying party, 426, 445
  relying party trust, 426
  resource partner organization, 426
  SAML (Security Assertion Markup Language), 423
sample federated Application
appVM, 441
IIS Manager, 442–443
PowerShell ISE, 441–442
token-signing certificate, 442
sample federated application, 441
publishing, 450–452
server role installation
adfsVM logon, 433–434
certificate import, 436
Configuration Wizard, 435
File Explorer, 436
Pre-requisite checks, 439
Review Options, 438
service account, 438
service name, 437
SQL Server database, 431
STS (Security Token Service), 423
WAP servers, 429
role service, 447–450
Web Application Proxy cluster, 430–431
web server, 430
WS-Federation and, 423
ADAC groups, creating, 372–373
Add Roles and Features Wizard, 21, 118, 227
ADFS (Active Directory Federation Services), 253
ADK (Assessment and Deployment Kit), 14
administrative access
JEA (Just Enough Administration), 315–316
role capability files, 316–317
LAPS (Local Administrator Password Solutions), 313
downloading, 314
PAW (Privileged Access Workstation), 312–313
domain controller security, 313
ADUC groups, creating, 372–373
Advisor, 542
AIA (Authority Information Access), 393
extensions, 398
aliases, 56
Always On VPN, 217–218
AMD Virtualization (AMD-V), 118
Applications and System logs, 28–29
AppLocker, 323–324
architecture
containers, 260
Hyper-V, 117
nested virtualization, 120
stretch clusters, 149–150
virtual machines, 260
[array] data type, 78
arrays, 61
cmdlets and, 98
ATA (Advanced Threat Analytics), 327–328
attach command, 269
attack evidence, 328–329
Audit Policy Settings, 330
advanced, 332–333
auditing, 329–332
AuditPol, 333
event log forwarding, 333–336
automated deployment, 11–12
DISM (Deployment Image Servicing and Management), 13–14
imaging, 12
SID, 12
Sysprep, 12–13
MDT (Microsoft Deployment Toolkit), 19
SIM (System Image Manager), 14–16
virtualization and, 19–20
WDS (Windows Deployment Services), 16–19
automatic variables, 83
Automation & Control (OMS), 541, 542
Azure Log Analytics, 542
Azure Operational Insights, 542
B
Backup & Recovery (OMS), 541, 543
BGP (border gateway protocol), 222
BIOS (Basic Input Output System), 4
BitLocker, 298–299
BitLocker Drive Encryption, 21
boot partitions, 8
BranchCache
Application Server content, 234
distributed cache mode, 233
File Server content, 234
Group Policy Object, 236
hosted cache mode, 233
installation, 235
Web Server content, 234
[byte] data type, 78
C
CA (Certificate Authority)
certificate auto-enrollment, 417–418
certificate templates, 406–417
built-in, 407
compatibility, 407–409
cryptography, 411–412
issuance requirements, 415–416
properties, 410
publishing certificates, 409–410
request handling, 410–411
requestors, 416–417
security, 413–414
database, 386
enterprise subordinate installation, 400–406
placement, 393
CAL (Client Access License), 3
casting data types, 77
CAU (Cluster-Aware Updating), 148–149
CCI (Configurable Code Integrity), 325
CDP (CRL Distribution Point), 393
extensions, 397
server configuration, 399–400
Certificate Authority (AD CS), 388
Certificate Authority Web Enrollment (AD CS), 389
Certificate Enrollment Policy Web Service (AD CS), 388
Certificate Enrollment Web Service (AD CS), 389
certificate templates, 406–407
built-in, 407
compatibility, 407–409
cryptography, 411–412
issuance requirements, 415–416
properties, 410
publishing certificates, 409–410
request handling, 410–411
requestors, 416–417
security, 413–414
certificates
AD FS, 432
policies, AD CS, 388
[char] data type, 77
checkpoints, virtual machines, 125
clearing variables, 84
CLI (command-line interface), 35
cloud, hybrid, 542
cluster upgrades, rolling, 117
clustering
categories
Active-Active, 137
Active-Passive, 137
multisite, 137
single-site, 137
failover, 134–136
application, 136, 138
categories, 137
clients, 136, 138
cluster storage, 138
components, 137–139
failback, 136
failover, 136
hardware, 139–140
high availability and, 135–136
management tasks, 144–145
migrating clusters, 141–142
network, 138
node management, 145–146
nodes, 136, 138
planned-versus unplanned, 146–147
properties, 145
quorum, 136, 138, 140–141, 147
resource, 138
roles, 143–144
scenarios, 139
service, 136, 138
shared storage, 136
terminology, 136
upgrading clusters, 141–142
Validation Wizard, 142–143
witness, 136, 138
guest clustering, 132–133
hardware, 139–140
host clustering, 132
networking, 147
SQL Server, instance installation, 461–465
stretch clusters, 137, 149–150
terminology, 136
types, 137
updates and, 148–149
cmldets, 38
arrays and, 98
ConvertTo-Csv, 67
ConvertTo-Html, 68–69
ConvertTo-Xml, 69–71
Export-Clixml, 71–73
ExportTo-Csv, 67
Format-List, 95–96
Format-Table, 96
Format-Wide, 94–95
function naming, 86
Get-Credential, 71–73
Get-EventLog, 49–51
Get-NetRoute, 182
Measure-Object, 62–63
Net-NetIPAddress, 182
New-NetRoute, 182
collections, 61
command line functions, 98
comparison operators
-eq, 76
-gte, 76
-gt, 76
-le, 76
-lt, 76
-ne, 76
operands, 75
regular expressions, 75
strings, 75, 77
Computer Management, 24
Conditional Access, 340
configuration
computer name, 9
Desktop Enterprise, 9
IPv4 address, 9
Server Core and, 10
Server Manager and, 9
time zone, 9
workgroups, 9
-Confirm parameter, 54–55
containers
architecture, 260
configuration
AD authentication, 280–281
default, 268–269
networking, 276–279
resources, 279–280
storage, 275–276
creating, 267–269
Docker, 263
installation, 264–265
hardware requirements, 263–264
host, 261
Internet connectivity and, 265
Hyper-V, 262–263
IIS and, 259
images, 261
automated creation, 271–274
customizing, 270–271
Docker Hub, 266–267
storage, 274–275
kernels and, 259
layers, 262
licensing, 264
limitations, 261
Linux, 263
memory, 264
microservices, 262
namespace isolation, 262
Nano Server, 261
operating-system image, 262
RD Session Hosts, 261
repository, 262
running, 267–269
sandbox, 261
Server Core, 261
software requirements, 263–264
VDI (Virtual Desktop Infrastructure), 261
virtual machines comparison, 260
containment operators
-contains, 81
-notcontains, 81
-contains containment operator, 81
ConvertTo-Csv cmdlet, 66–67
ConvertTo-Html cmdlet, 68–69
ConvertTo-Xml cmdlet, 69–71
create command, 269
Create Virtual Switches page, 118
Credential Guard, 296–297
credentials
encrypting, 71–73
saving, to XML files, 73–74
cryptography, certificate templates, 411–412
CSP (Certificate Practice Statement), 390
CSVs (Cluster Shared Volumes), 152–155
D
Dashboard, Server Manager, 23–24
data, importing, to PowerShell, 74
data at rest
BitLocker, 298–299
EFS (Encrypting File System), 297–298
data deduplication
data optimization, 162–163
background operations, 164
reading data, 163–164
enabling, 164–165
excluding files, 165–166
minimum file size, 166
 scheduling, 165
 shared folders, 162
 software installation data, 162
 space-saving technologies, 161
 virtualization files, 162
data in transit, Windows Firewall with Advanced Security, 300–302
 inbound rules, 302–303
 outbound rules, 302–303
Data Protection Manager (System Center)
 server, hardware requirements, 459
 upgrade path, 458
data types
 [array], 78
 [byte], 78
 casting, 77
 [char], 77
 [DateTime], 78
 [decimal], 78
 [double], 78
 [hashtable], 78
 [int], 78
 -is operator, 79–80
 [long], 78
 [single], 78
 [string], 77
 [void], 78
 [xml], 78
databases, System Center
 cluster recommendations, 459–460
 file types, 460
Datacenter Firewall, 222
 [DateTime] data type, 78
 DCDiag, 202
debugging, DNS and, 200–201
 [decimal] data type, 78
 DEP (Data Execution Prevention), 118
 DES (Data Encryption Standard), 293
 Desktop Enterprise
 configuration, 9
 installation, 7
Device Guard, 119, 324
 CCI (Configurable Code Integrity), 325
 configuration, 325–327
 Platform and UEFI Secure Boot, 325
 Virtual Secure Mode, 325
 Virtual Secure Mode Protected Code Integrity, 325
 Device Manager, 24–25
 devices, discrete, 124
 DFS (Distributed File System), 229
 DFS Management console
 Diagnostic Reports Wizard, 243
 Health Report, 244
 Propagation report, 244
 Propagation Test, 244
 PowerShell commands, 244
 Verify Topology tool, 244
DFS Namespaces, 237
 DFS Replication, 242
 Domain-Based Namespaces, 238
 folders, 238
 shared, 238–241
 targets, 238
 installation, 239–240
 Namespace Root, 238
 Namespace Server, 238
 network ports, 245
 PowerShell and, 240
 Stand-Alone Namespaces, 238
DFS Replication
 configuration, 241–243
 installation, 241
DHCP (Dynamic Host Configuration Protocol), 179
 database, backups, 209–210
 DHCPFDiscover packet, 202
 failover relationships, 208–209
 filters, 207
 high availability and, 208–209
 IPv4 configuration, 181
 policies, 207
 Relay Agent, 202
 reservations, 205
 scopes, 204–205
 multicast scope, 206
 options, 206
 superscope, 205
 server role, installation, 203
 servers, rogue, 203
 Diagnostic Reports Wizard, 243
differencing disks, 121
 DirectAccess, 218
 VPN and, 211
discrete devices, 124
disk partitioning, planning, 5
 DISM (Deployment Image Servicing and Management), 13–14
 DNS (Domain Name Service), 179
cashing, 195
DCDiag, 202
debbugging, 200–201
Dig, 201
domain controllers, 188
dynamic, 188
KSK (key signing key), 198
monitoring, 199–200
name resolution processing, 192
  advanced settings, 195–196
non-authoritative resolution, 192–194
Nslookup, 201
Performance Monitor and, 200–201
policies, 196–197
records
  AAAA (host), 189
  CNAME (alias), 189
  A (host), 189
  MX (mail exchanger), 189
  NS (name server), 189
  removing, 197–198
  scavenging, 197
  SRV (service location), 189
  TXT (text), 189
security, 198–199
SRV (Service Location), 188–189
troubleshooting, 201–202
zones, 189–192
  creating, 190–192
ZSK (zone signing key), 198
Docker, 263
commands
  attach, 269
  create, 269
  exec, 269
  pause, 269
  ps, 269
  rm, 269
  start, 269
  stop, 269
  unpause, 269
DockerMsftProvider, 264
DockerProvider, 264
installation, 264–265
provider download, 265
Docker Hub, container images, 266–267
dockerfiles, 271–272
  image creation, 273
PowerShell, 274
domain controllers, 353
auditing, 360–362
  counts, 354
  forest root, 354
Global Catalog servers, 354
installation, type, 355–357
logging, 360–362
operating system, 354–355
operating system components, 362–363
placement, 354
Remote Desktop, 363
Remote Management, 363
SRV records, 189
UAC (User Account Control), 363
Windows Defender, 363
Windows Firewall, 363
[dual] data type, 78
dynamic IP addresses, DHCP and, 202
dynamic quorum, 140–141
dynamic witness, 141
dynamically quorum, 140–141
dynamically expanding virtual hard disks, 120

E
EAP (Extensible Authentication Protocol), 215–216
EFI system partition, 8
EFS (Encrypting File System), 297–298
certificate templates, 412–413
e-mail, PKI (public key infrastructure) and, 392
encrypting
  credentials, 71–73
  FEK (file encryption key), 298
  VMK (volume master key), 299
encryption, PKI (public key infrastructure) and, 392
enterprise assurance licensing, 4
e-mail, PKI (public key infrastructure) and, 392
environment variables, 84–85
-eq comparison operator, 76
-eq operator, 75
ESAE (Enhanced Security Administrative Environment), 318
  locked-down accounts, 319
  selective authentication, 319
ethical hacking, 288
  penetration testing, 288
Event Viewer, 28–29
events, objects, 60
exec command, 269
Export-Clixml cmdlet, 71–73
exporting, credentials, 71–73
ExportTo-Csv cmdlet, 67
expressions, regular expressions, comparison operators, 75
Failover Clustering, 21
failover clustering, 134–136
application, 136
categories, 137
clients, 136
components
  application, 138
  clients, 138
  cluster storage, 138
  network, 138
  nodes, 138
  quorum, 138
  resource, 138
  service, 138
  witness, 138
failback, 136
failover, 136
hardware, 139–140
high availability and, 135–136
Hyper-V, 151–152
  CSVs, 152–155
  implementing, 152–154
Hyper-V Replica, 131
management tasks
  cluster networks, 144
  cluster nodes, 144
  cluster permissions, 144
  configuration new services, 145
  migrating services, 145
  quorum settings, 145
  removing clusters, 145
migrating clusters, 141–142
nodes, 136
  managing, 145–146
planned versus unplanned, 146–147
properties, 145
quorum, 136, 147
  dynamic, 140–141
  no majority, 140
  node and disk majority, 140
  node and file share majority, 140
  node majority, 140
roles
  DFS Namespace Server, 143
  DHCP Server, 143
  DTC (Distributed Transaction Coordinator), 143
  file server, 144
generic application, 144
generic script, 144
generic service, 144
Hyper-V Replica Broker, 144
iSCSI Target Server, 144
iSNS Server, 144
Message Queuing, 144
Other Server, 144
Virtual Machine, 144
WINS Server, 144
scenarios, 139
service, 136
shared storage, 136
SQL Server, installation, 462–464
terminology, 136
upgrading clusters, 141–142
Validation Wizard, 142–143
witness, 136
Failover Clustering Management console, live
migration, 128
failover relationships, DHCP and, 208–209
FEK (file encryption key), 298
File and iSCSI Services, 228
File and Storage Services, 227
  DFS Namespaces, 237
  File and iSCSI Services, 228
file server
  design concepts, 229
  permissions, assigning, 231–232
File Server component
  file shares, creating, 230–231
  installation, 229
File Services, 227
disaster recovery, 229
  high availability, 229
  number of users, 229
  security, 229
  server placement, 229
file shares, 255
file systems
  NTFS (New Technology File System), 157
    change journal, 158
    ReFS comparison, 159–161
    reparse points, 158
    sparse file support, 158
  ReFS (Resilient File System), 157, 159
    block cloning, 159
    integrity streams, 149
    NTFS comparison, 159–161
files
  BranchCache, 232–233
    Application Server content, 234
distributed cache mode, 233
File Server content, 234
Group Policy Object, 236
hosted cache mode, 233
installation, 235
Web Server content, 234
dockerfile, 271–272
image creation, 273
filtering, 74–75
DHCP filters, 207
MAC addresses and, 207
wildcards, 207
firewalls, 185–186
Datacenter Firewall, 222
fixed-size virtual hard disks, virtual machines, 120
folders, shared, DFS Namespaces, 238–241
fonts, PowerShell, 37
for loop, 96–97
foreach loop, 97–99
Format-List cmdlet, 95–96
formats, objects, converting, 66
Format-Table cmdlet, 96
formatting, output
  Format-List cmdlet, 95–96
  Format-Table cmdlet, 96
  Format-Wide cmdlet, 94–95
Format-Wide cmdlet, 94–95
FSRM (File Server Resource Manager), 245
  Classification Management
    Classification Properties, 248
    Classification Rules, 248
  console, 247
disk usage templates, 251
features deployment, 246–247
File Classification Infrastructure, 245
File Management Tasks, 245–246
  Action option, 249
  Condition option, 250
  General option, 249
  Notification option, 249
  Report option, 249
  Schedule option, 250
  Scope option, 249
File Screening Management, 246, 251–252
installation, 246
options
  Access-Denied Assistance, 248
  Automatic Classification, 248
  Email Notifications, 247
  File Screen Audit, 248
  Notification Limits, 247
Report Locations, 248
Storage Reports, 248
Quota Management, 246
  quota templates, 250
  quotas, 250
Storage Reports, 246
functions
  creating, command lines and, 98
  naming, cmdlets, 86
PowerShell
  creating, 85, 86–88
  Get-Help About Functions, 85
  parameters, 88–93
  pipeline objects, 93
  pseudocode, 87
  splatting, 86
  viewing all, 94
G
  gateway-to-gateway tunneling, IPsec and, 304
  ge comparison operator, 76
  Generation 2 virtual machine, 123
Get-Credential cmdlet, 71–73
Get-Credential dialog box, 72
Get-Eventlog cmdlet, 49–51
GPO (Group Policy Object), 374
  account policies, 293–294
  Domain Password policy, 293–294
  Domain-Account Lockout policy, 294
  links, PowerShell and, 380
  reports, 378–379
  searching for, 377–378
  settings, PowerShell and, 379–380
GRE (Generic Routing Encapsulation), 222
Group Policy, 373, 374
cmdlets
  Backup-GPO, 376
  Copy-GPO, 376
  Get-GPInheritance, 376
  Get-GPO, 376
  Get-GPOReport, 376
  Get-GPPermission, 377
  Get-GPPrefRegistryValue, 377
  Get-GPRegistryValue, 377
  Get-GPResultantSetOfPolicy, 377
  Get-GPStarterGPO, 377
  Import-GPO, 377
  Invoke-GPUpdate, 377
  New-GPLink, 377
  New-GPO, 377
New-GPStarterGPO, 377
Remove-GPLink, 377
Remove-GPO, 377
Remove-GPPrefRegistryValue, 377
Remove-GPRegistryValue, 377
Rename-GPO, 377
Restore-GPO, 377
Set-GPInheritance, 377
Set-GPLink, 377
Set-GPPermission, 377
Set-GPPrefRegistryValue, 377
enforcement, 376
tasks, 376–377
troubleshooting, 380–382
Group Policy Editor, user accounts, 289–292
Group Policy Management Editor, GPO
(Group Policy Object)
account policies, 293–294
Domain Password policy, 293–294
Domain-Account Lockout policy, 294
groups (Active Directory), 370
creating, 372–373
distribution, 371
members, adding, 373
scopes, 371
security, 371
token sizes, 371–372
-gt comparison operator, 76
guest operating systems, 116
GVLK (generic volume license key), 11

H
hacking
ethical, 288
penetration testing, 288
hard disks, virtual
differencing, 121
dynamically expanding, 120
fixed size, 120
pass-through, 121
recommendations, 121
hardening the system, 327–328
hardware
containers, 263–264
failover clustering, 139–140
[hashable] data type, 78
high availability
DHCP and, 208–209
failover clustering and, 135–136
host resources, protection, 117
hybrid cloud, 542
Hyper-V, 2, 19–20, 115–116
AMD Virtualization (AMD-V), 118
architecture, 116
clustering
failover, 151–154
guest clustering, 132–133
host clustering, 132
configuration, 121–126
containers, 262–263
DEP (Data Execution Prevention), 118
failover clustering, 134–136
categories, 137
components, 137–139
hardware, 139–140
high availability and, 135–136
terminology, 136
high-availability option, 132
host computer, 115
host resource protection, 117
Hyper-V Manager functionalities, 117
installation, 118–119
PowerShell and, 119
prerequisites, 118
Intel VT (Virtualization Technology), 118
machine activation, 20
networking, 121–122
RDMA (Remote Direct Memory Access), 122
virtual switches, 121–122
VMQ (virtual machine queue), 122
new features, 116–117
virtual machines, 117–118
New-VHD PowerShell cmdlet, 120
NLB (Network Load Balancing), 133–134
partitioning, 120
PowerShell Direct, 116
PowerShell Direct and, 112
rolling cluster upgrade, 116
SLAT (second-level address translation), 118
start order priority, 117
storage, 120
storage QoS (Quality of Service), 117
virtual hard disks, 120–121
virtual machines
checkpoints, 125
configurations, 122–123
discrete devices, 124
exporting, 125–126
importing, 125–126
integration services, 124
live migration, 126
I

identity federation, 424
  Microsoft Office 365 and, 424
  Salesforce and, 424
iDNS (internal DNS Service), 224
IDS (intrusion detection system), ATA, 327
if loop, 99–100
IIS (Internet Information Services), 259
  entrypoint, 268
IKEv2 (Internet Key Exchange v2 Tunneling Protocol), 212
images
  containers, 261
    automated creation, 271–274
    customizing, 270–271
    Docker Hub, 266–267
    storage, 274–275
  deploying, 18–19
    WDS (Windows Deployment Services), 16
importing, to PowerShell, 74
-is operator, 81–82
input operations, 65–66
Insights & Analytics (OMS), 541, 542
installation
  automated deployment, 11–12
    DISM, 13–14
    imaging, 12–13
    MDT, 19
    SIM, 14–16
    virtualization and, 19–20
    WDS, 16–19
Desktop Enterprise, 7
drivers, 4
firmware
  BIOS, 4
  UEFI, 4
Hyper-V, 118–119
  location, 8
  Server Core, 7, 355–357
  steps, 5–9
  type, 7, 355–357
virtual machines, 5
[int] data type, 78
integration services, 124
Intel VT (Virtualization Technology), 118
IP (Internet Protocol), 179
  configuration, 180–182
  Ping utility and, 181
IPsec
  configuration
    firewall rules, 309–310
    GPO and, 308–309
      Windows Firewall administration, 310–311
  connection security rules, 305–306
  authentication exemption, 305
  authentication method, 307–308
  custom, 306
  isolation, 305
  Requirements page, 306–307
  Server to Server, 306
  tunnel, 306
modes, 305
  transport mode, 305
  tunnel mode, 305
monitoring
  Main Mode, 311
  Quick Mode, 312
uses, 304
IPv4, configuration, 180–182
IPv6, configuration, 181–182
-is operator, data type verification, 79–80

J

JEA (Just Enough Administration), 341
role-capabilities
  AliasDefinitions, 316
  AssembliesToLoad, 316
  EnvironmentVariables, 316
  FormatsToProcess, 316
  FunctionDefinitions, 316
  ModulesToImport, 316
ScriptsToProcess, 316
TypesToProcess, 316
VariableDefinitions, 316
VisibleAliases, 316
VisibleCmdlets, 316
VisibleExternalCommands, 316
VisibleFunctions, 316
VisibleProviders, 316
session-configuration files
RoleDefinitions, 317
RunAsVirtualAccount, 317
RunAsVirtualAccountGroups, 317
SessionType, 317
TranscriptDirectory, 317
JIT (Just In Time) administration, 341

K
Kerberos, long-term keys, 294–295
kernels, containers and, 259
KMCI (kernel mode code integrity), 325
KMS (Key Management Service), 10–11

L
L2TP (Layer 2 Tunneling Protocol), 212
LACP (Link Aggregation Control Protocol), NIC
  Teaming and, 185
  latency, VPNs and, 210
-le comparison operator, 76
licensing
  CAL (Client Access License), 3
core-based, 3
  enterprise agreement, 4
  GVLK (generic volume license key), 11
OEM (Original Equipment Manufacturer), 3
  software assurance, 4
  virtualization, 3
  volume, 3–4
-like operator, 76–77
Linux, containers, 263
live migration, 126
  cleanup, 128
  guest-memory transfer, 128
  requirements, 128–129
  setup, 128
  shared-nothing live migration, 128
  state transfer, 128
  virtual machines, 127–128
load balancing, networks, 219–220

LOB (line-of-business) applications, 36
logs
  Application and System logs, 28–29
debugging, DNS and, 200–201
-long data type, 78
loops, PowerShell
  for, 96–97
  foreach, 97–99
  if, 99–100
  switch, 100–102
  Where-Object method, 104–108
while, 102–104
LSA (Local Security Authority), 371–372
  -It comparison operator, 76

M
MAC address spoofing, virtual machines, 119
MAC addresses, filtering and, 207
MAK (Multiple Activation Key), 10
malware, 287
  AppLocker and, 323–324
  Device Guard, 324
  CCI (Configurable Code Integrity), 325
  configuration, 325–327
  Platform and UEFI Secure Boot, 325
  Virtual Secure Mode, 325
  Virtual Secure Mode Protected Code Integrity, 325
SRPs (Software Restriction Policies), 323
  mandatory parameters, 90–91
MDT (Microsoft Deployment Toolkit), 19
Measure-Object cmdlet, 62–63
memory, containers, 264
methods, objects, 60
migration
  clusters, 141–142
  live migration, 126
    cleanup, 128
    guest-memory transfer, 128
    requirements, 128–129
    setup, 128
    shared-nothing live migration, 128
    state transfer, 128
    virtual machines, 127–128
virtual machines, 126–127
  Exporting and Importing Virtual Machines, 127
  Live Migration, 127
Quick Migration, 127
Virtual Machine and Storage Machine, 127
MIM (Microsoft Identity Manager), 341
monitoring
Event Viewer, 28–29
Performance Monitor, 32–33
Resource Monitor, 30–32
System Center Operations Manager, 27
Task Manager, 29–30
Multifactor Authentication, 340

N
named parameters, 88–90
NDES (Network Device Enrollment Service)
(AD CS), 389
-ne comparison operator, 76
nested virtualization, 117, 119–120
.NET Framework, 21
network adapter teaming, 182–183
NIC teaming, 183–184
LACP, 185
load-balancing modes, 185
Static Teaming mode, 185
Switch Independent mode, 185
virtualization hosts and, 183
Network Controllers, 221
NETWORK SERVICE account, 27
networks
cluster, 147
containers, 276–279
files, BranchCache, 232–237
load balancing, 219–220
New-VHD PowerShell cmdlet, 120
NIC teaming, 183
LACP, 185
load-balancing modes
Address Hash, 185
Dynamic, 185
Hyper-V Port, 185
new teams, 184
Static Teaming mode, 185
Switch Independent mode, 185
NLB (Network Load Balancing), 179, 219–220
-notcontains containment operator, 81
-notin operator, 81–82
NPS (Network Policy Server), 215–217
Nslookup, 201
NTFS (New Technology File System), 157
change journal, 158
ReFS comparison, 159–161
reparse points, 158
sparse file support, 158
NTLM (NT LAN Manager), 294–295
O
objects
arrays, 61
collections, 61
credential, encrypting, 71–73
events, 60
filtering, 74–75
comparison operators, 75–76
wildcards, 76–77
format conversion, 66
measuring, 62–63
members, 59–60
methods, 60
properties, 59–60
selecting, 63–65
sorting, 61–62
as table, 61–62
OEM (Original Equipment Manufacturer)
licensing, 3, 10
OMS (Operations Management Suite), 541
Automation & Control, 541, 542
Backup & Recovery, 541, 543
browsers supported, 546
history, 542
Insights & Analytics, 541, 542
Log Analytics, 546–552
onboarding, 546–550
portal link, 550
pricing, SLA, 543–544
Query Language
event queries, 554–555
performance queries, 552–554
Security & Compliance, 541, 543
Security and Audit Solution, 551
Solutions Gallery, 551
system requirements
connected sources, 545
data sources, 545
URL access, 546
one-liners, 373
Online Responder (AD CS), 389
OOBE (Out-of-Box Experience), 12
operands, 75
operating systems

domain controllers, 354–355

guest, 116

Operations Manager (System Center)

activation, 495

agents, 483

databases, 482

Data Warehouse database, 483

retention period, 483

StandardDatasetAggregation table, 483

installation

activation, 495

administration rights, 492

Diasgnostic and Usage Data, 493

initial screen, 486–487

license terms, 488–489

location, 487

management group name, 488

operational database configuration, 489–490

Operations Manager shell, 494

Reporting Services instance, 490–491

results window, 494

SCOM features, 487

service accounts configuration, 492

summary page, 493

web console, 491

management packs, 484

management server

Config Service, 482

Health Service, 482

RMSE (Root Management Server Emulator), 482

SDK Service, 482

prerequisites, 484

passing, 488

web console, 485

Report Viewer, installation, 485

server, hardware requirements, 459

services

Config Service, 483–484

Health Service, 484

Microsoft Monitoring Agent, 483, 484

SDK Service, 483, 484

SQL CLR Types, installation, 485

upgrade path, 458

web console, 485

Windows Server management pack

importing management packs, 496–498

selecting for install, 498–499

operators

> (redirection), 65

comparison operators

-eq, 76

-ge, 76

-gt, 76

-le, 76

-lt, 76

-ne, 76

regular expressions, 75

strings, 75

containment operators

-contains, 81

-notcontains, 81

-eq, 75

-in, 81–82

-is, 79–80

-like, 75

-notin, 81–82

operands, 75

-replace, 82

Ops Insights, 542

Orchestrator (System Center), upgrade path, 458

OU (organizational unit), creating, 351–353

Out-File command, 65

output, formatting

Format-List cmdlet, 95–96

Format-Table cmdlet, 96

Format-Wide cmdlet, 94–95

output operations, 65–66

P

packet sniffers, 202

PAM (Privileged Access Management), 319

Administrative Forest, 320

JEA (Just Enough Administration), 341

JIT (Just In Time) administration, 341

MIM (Microsoft Identity Manager), 320, 341

MIM Portal, 321

MIM Service, 321

MIM Service Database, 321

PAM Client, 320

PAM Component Service, 320

PAM Monitoring Service, 320

PAM REST API, 320

Production Forest, 320

parameters

-Confirm, 54–55

mandatory, 90–91
named, 88–90
positional, 91–92
switch, 92–93
values, passing multiple, 51–52
-WhatIf, 53–54
parenthetical commands, 52
partitioning
boot partitions, 8
EFI system partition, 8
recovery partition, 8
system partitions, 8
pass-the-hash, 294
pass-the-ticket attacks, 296–297
pass-through virtual hard disks, 121
pause command, 269
penetration testing, 288
Performance Monitor, DNS and, 200–201
permissions, assigning, 231–232
phishing, 287
simulation, 288
Ping utility, IP and, 181
pipelines, 59
objects, selecting subsets, 63–65
PKI (public key infrastructure)
certificate policies, 390
certificates, 388
issuing, 387
CSP (Certificate Practice Statement), 390
documentation, 389–390
email services and, 392
encryption and, 392
environment management, 392
HTTPS and, 387
intermediate CA, 388
issuing CA, 388
LDAPs and, 387
policies and procedures, 388
primary components, 387–388
root CA, 387–388
offline, 394–396
templates, 388
tiers
four-tier hierarchy, 392
single-tier hierarchy, 391
three-tier hierarchy, 391
two-tier hierarchy, 391
two-tier hierarchy implementation, 393–406
web services and, 392
point-to-site VPN, 222
positional parameters, 91–92
PowerShell, 35–36, 45
32-bit version, 36–37
64-bit version, 36–37
About files, 55–56
AD (Active Directory), replication and, 350
aliases, 44–46, 56
Begin statement, 93
CLI and, 35
CMD.EXE-EXE-EXE-like commands, 44–46
cmdlets, 38
auditing logs, 335
dialog boxes, 52–53
Get-Eventlog, 49–51
spaces in, 51
syntax, 49–51
Windows Firewall and Advanced
Security, 303
commands, 58–59
saving results, 65
shortened syntax, 56–58
console, customization, 37
ConvertTo-Csv cmdlet, 66–67
ConvertTo-Html cmdlet, 68–69
ConvertTo-Xml cmdlet, 69–71
credentials, encrypting, 71–73
cutting, 37–38
data types
[array], 78
[byte], 78
casting, 77
[char], 77
[DateTime], 78
[decimal], 78
,double], 78
[hashable], 78
[int], 78
-is operator, 79–80
[long], 78
[single], 78
[string], 77
(void], 78
[xml], 78
DFS Namespaces, 240
Dir /S, 45
dockerfiles, 274
End statement, 93
execution policies, 43
Export-CIxml cmdlet, 71–73
ExportTo-Csv cmdlet, 67
fonts, 37
forward compatibility, 36
functions
  creating, 85, 86–88
  Get-Help About Functions, 85
parameters, 88–93
pipeline objects, 93
pseudocode, 87
splatting, 86
viewing all, 94
GPO links, 380
GPO settings, 379–380
GUI and, 35
help
  Get-Help, 46–47
  Get-Help updates, 47–48
  online files, 48–49
Hyper-V installation, 119
importing to, 74
input operations, 65–66
-like operator, 76–77
LOB applications, 36
loops
  for, 96–97
  foreach, 97–99
  if, 99–100
  switch statement, 100–102
  Where-Object method, 104–108
while, 102–104
Measure-Object cmdlet, 62–63
network, configuration, 182
objects
  arrays, 61
  collections, 61
  events, 60
  members, 59–60
  methods, 60
  properties, 59–60
  selecting, 63–65
  sorting, 61–62
  as table, 61–62
operators
  > (redirection), 65
  comparison, 75–76
  comparison operators, 75, 76
  containment operators, 81
  -eq, 75
  -in, 81–82
  -is, 79–80
  -like, 75
  -notin, 81–82
  operands, 75
  -replace, 82
Out-File command, 65
output operations, 65–66
parameters
  -Confirm, 54–55
  multiple values, 51–52
  -WhatIf, 53–54
pasting, 37–38
pipelines, 59
Process statement, 93
remote systems
  commands, 110–111
  Enable-PSRemoting, 109
  persistent connections, 111–112
  PowerShell Direct, 112
  scripts, 111
  workgroup servers, 110
Run As Administrator, 37
selections, 38
Select-Object cmdlet, 63–65
Service object, properties, 60
sessions, recording, 44
Show-Command, 52–53
transcription operations, 44
user accounts
  deleted, restoring, 370
  reports, 368–369
  stale, 369–370
variables
  automatic, 83
  clearing, 84
  environment variables, 84–85
  preference, 83
  removing, 84
  user-created, 83
  Variable: drive, 84
wildcards, 76–77
PowerShell Direct, 112, 117
virtual machines, 126
PowerShell ISE
(Integrated Scripting Environment), 36, 38
cmdlets, 38
colors, 40
Command add-on, 38
Command pane, 38–39
fonts, 40
General Settings tab, 40, 41
Intellisense, 40–41
Options dialog box, 40
profiles, 41–42
editing, 42–43
Script pane, 39
Tools, 39–40
PPTP (point-to-point tunneling protocol), 211
preference variables, 83
privileged access, Group Policy Editor, 289–292
privileges, delegating, 295–296
processes, finding all running, 104–108
processors, core-based licensing, 3
profiles, PowerShell ISE, 41–42
editing, 42–43
properties
objects, 59–60
Service object
CanShutdown, 60
MachineName, 60
StartType, 60
Protected Users groups, 294–295
protocols, VPNs
IKEv2, 212
L2TP, 212
PPTP, 211
SSTP, 212
ps command, 269
pseudocode, 87
Q
QoS (Quality of Service)
storage, 157
Hyper-V, 117
Storage QoS, 176
quorums, dynamic, 140–141
R
RADIUS (Remote Access Dial-In Service), 215–217
ransomware, 287
RAS (Remote Access Server)
DirectAccess, 211
routing, 211
RAS Gateway, 221–222
RDMA (Remote Direct Memory Access), 122
SET and, 223
RDS (Remote Desktop Services), 210
recovery partition, 8
recursive searches, 44
redirection (>) operator, 65
ReFS (Resilient File System), 157
block cloning, 159
integrity streams, 159
NTFS comparison, 159–161
regular expressions, comparison operators, 75
remote access, 210–211. See also RAS (Remote Access Server)
NPS (Network Policy Server), 215–217
RADIUS (Remote Access Dial-In Service), 215–217
RDS (Remote Desktop Services), 210
VPNs (virtual private network), 210
WAP (Web Application Proxy), 211, 218–219
Remote Desktop, domain controllers and, 363
Remote Management, domain controllers and, 363
remote systems, PowerShell
commands, 110–111
Enable-PSRemoting, 109
persistent connections, 111–112
PowerShell Direct, 112
scripts, 111
workgroup servers, 110
removing variables, 84
-replace operator, 82
Replicate Folder Wizard, 242
replication, AD (Active Directory),
PowerShell and, 350
resource metering, 124
Resource Monitor, 30–32
resources, containers, 279–280
reverse lookup zones, 189–190
rm command, 269
rolling cluster upgrades, 117
root CA, 387–388
offline, 394–396
configuration, 396–399
routing, RAS and, 211
Routing and Remote Access dialog box, 214
RSAT (Remote Server Administration Tools), 7
S
SAM (Security Accounts Management), 179
SAML (Security Assertion Markup Language), 423
SANs (storage area networks), 157
saving
command results, 65
credentials, to XML files, 71–73
scalar input, 80
SDN (Software Defined Network)
SDNS (SDN Services), 221
iDNS (internal DNS Service), 224
SET (Switch Embedded Teaming), 223
SLB (Software Load Balancing)
  DIP (Dynamic IP address), 223
  MUX (SLB Multiplexer), 223
  VIP (Virtual IP address), 223
SDN (Software Defined Networking), 179, 220–221
  Datacenter Firewall, 222
  Hyper-V Network Virtualization, 221
  Network Controller, 221
  RAS Gateway, 221–222
searches
  recursive searches, 44
  wildcards, 76–77
secure, 285–286
administrative access
  JEA (Just Enough Administration), 315–318
  LAPS (Local Administrator Password Solutions), 313, 314
  PAW (Privileged Access Workstation), 312–313
anti-malware software, 286
attack surface area, 287
attack vectors, 287
attacks, evidence, 328–336
data at rest
  BitLocker, 298–299
  EFS, 297–298
encryption, FEK, 298
GPO (Group Policy Object)
  account policies, 293–294
  Domain Password policy, 293–294
  Domain-Account Lockout policy, 294
Group Policy Management Editor, GPO
  (Group Policy Object), 293–294
hacking, ethical, 288
hardening system, ATA (Advanced Threat Analytics), 327–328
IPsec
  configuration, 308–311
  connection security rules, 305–308
  modes, 305
  monitoring, 311, 312
  uses, 304
malware, 287
  AppLocker and, 323–324
  Device Guard, 324–327
  protection, 322–327
  SRPs, 323
  pass-the-hash attacks, 294
  pass-the-ticket attacks, 296–297
penetration testing, 288
permissions
  admin, 286
  users, 286
phishing, 287
ransomware, 287
risks, 286–287
social engineering, 287
Trojans, 287
updates, 286
user accounts, 288, 292–293
  Active Directory Users and Computers, 292–293
  Credential Guard, 296–297
  privileged access, 289–292
  Protected Users groups, 294–295
user credentials, 286
viruses, 287
Windows Firewall, 286
Security & Compliance (OMS), 541, 543
security boundaries, 342
Select-Object cmdlet, 63–65
Server Core, 355–357
  configuration and, 10
  installation, 7
  PowerShell and, 7
Server Manager, 227
  configuration and, 9
  Dashboard view, 23–24
  features, 21–23
  File and Storage Services, 230
  monitoring, 23–24
  roles, 21–23
SERVICE account, 27
Service Management Automation (System Center), upgrade path, 458
Service Manager (System Center)
  server, hardware requirements, 459
  upgrade path, 458
Service object, properties
  CanShutdown, 60
  MachineName, 60
  StartType, 60
Service Provider Foundation (System Center), upgrade path, 458
SET (Switch Embedded Teaming), 223
shared-nothing live migration, 128
shielded virtual machines, 1, 123–124
shortened command syntax, 56–58
Show-Command (PowerShell), 52–53
sign-on offline, 294–295
SIM (System Image Manager), 14–16
configuration passes, 15
[single] data type, 78
site system roles (System Center)
  Application Catalog web service point, 503
  Application Catalog website point, 503
certificate registration point, 503
cloud-based distribution point, 503
component provider, 502
configurations supported, 504
distribution point, 503
endpoint protection point, 503
enrollment point, 503
enrollment proxy point, 503
fallback status point, 503
management point, 503
reporting services point, 503
services connection point, 503
SMS provider, 502
software requirements, 503–504
software update point, 503
state migration point, 503
site-to-site tunneling, IPsec and, 304
site-to-site VPN, 222
SLAs (Service Level Agreements), OMS, 543–544
SLAT (second-level address translation), 118
SLB (Software Load Balancing), 222–223
  DIP (Dynamic IP address), 223
  MUX (SLB Multiplexer), 223
  VIP (Virtual IP address), 223
smart paging, 124
SMB (Server Message Block), 128
SMD Direct, 122
social engineering, 287
software assurance licensing, 4
Software Defined Networking, 2
splattering functions, 86
spoofing, MAC addresses, virtual machines, 119
SQL Server
  failover cluster, installation, 462–464
  Instance Configuration, 462–463
  instances, installation in cluster, 461–465
  System Center, file types, 460
SQL Server Installation Center, 461–462
SRPs (Software Restriction Policies), 323
SRV (Service Location), 188–189
  records, domain controller, 189
SSTP (Secure Socket Tunneling Protocol), 212
start command, 269
start order, priority, 117
Static Teaming mode, NIC Teaming, 185
stop command, 269
storage
  container images, 274–275
  containers, 275–276
data deduplication, 157
  advanced settings, 165–166
  background and, 164
  enabling, 164–165
  optimization and, 162–163
  reading optimized data, 163–164
  shared folders, 162
  software installation data, 162
  space-saving technologies, 161–162
  virtualization files, 162
domain controllers, 359–360
file systems, 157
  NTFS (New Technology File System), 157–161
  ReFS (Resilient File System), 157, 159–161
storage QoS (Quality of Service), 157
Storage Replica, 157
Storage Spaces, 157
Storage QoS (Quality of Service), 157
dedicated policy, 176–177
aggregated policy, 176–177
Storage Replica, 2, 170–171
  AD DS and, 174
  asymmetric storage, 171
  asynchronous replication, 171, 173
  Datacenter Edition and, 174
  deployment, 174–176
  DFS (Distributed File System), 170
  network connectivity and, 174
  replication options, 172
  storage and, 174
  stretch clusters, 171
  symmetric storage, 171
  synchronous replication, 171
Storage Spaces, 166–167
  continuous availability, 168
  CSVs (Cluster Shared Volumes), 166
resilience
  mirroring, 167
  parity, 167
  simple, 167
storage tiering, 168
write-back cache, 168
Storage Spaces Direct, 2, 168
LAN (Local Area Network), 169
local storage, 169
servers, 169
SMB, 169
stretch clusters, 137, 149–150
Storage Replica, 171
[string] data type, 77
strings
	comparison operators, 75, 77
	-match operand, 80–81
STS (Security Token Service), 423
Switch Independent mode, NIC Teaming, 185
switch parameters, 92–93
switch statement, loops, 100–102
csync shares, 255
syntax, commands, shortened, 56–58
Sysprep, 12–13
	virtualization and, 12–13
SYSTEM account, 27
System Audit Mode, 13
System Center, 457
Advisor, 542
Configuration Manager
boundaries, 526–527
boundary groups, 526–530
branches, 499–501
Client Push Installation method, 530–531
client settings, 532–534
collections, 535–536
Computer Agent, 532
configuration, 517–526
discovery methods, 518–521
disk space recommendations, 505
hardware inventory cycle, 532
hardware recommendations, 505
primary site servers, 506–517
server hardware, 459
site servers, 501–502, 505–517
site system roles, 502–504
software inventory cycle, 533
upgrade path, 458
Data Protection Manager
server hardware, 459
upgrade path, 458
install sequence
database clusters, 459–460
database file types, 460
hardware, 459
SQL Server version, 459

Operations Manager
activation, 495
agents, 483
databases, 482–483
installation, 486–495
management packs, 484
management server, 482
prerequisites, 484, 485, 488
Report Viewer, 485
server hardware, 459
services, 483–484
SQL CLR Types, 485
upgrade path, 458
web console, 485
Windows Server management pack, 496–499
Orchestrator
server hardware, 459
upgrade path, 458
Service Management Automation,
upgrade path, 458
Service Manager
server hardware, 459
upgrade path, 458
Service Provider Foundation, upgrade path,
458
SQL Server
database clusters, 459–460
database file types, 460
instance installation in cluster, 461–465
upgrade sequence, 457–458
VMM (Virtual Machine Manager), 20,
465–466, 470
compute fabric, 470
configuration, 466–469
DHCP (Dynamic Host Configuration
Protocol), 470–471
DNS (Domain Name System), 470
host groups, 470
Hyper-V, 470
infrastructure servers, 470–472
installation, 466–469
library, 470
network fabric, 472–476
server hardware, 459
storage fabric, 476–477
upgrade path, 458
virtual machines, 478–481
VMware vCenter servers, 470
VMware vSphere host, 470
System Center Configuration Manager
(System Center)
- boundaries, 526–527
  - creating, 527
- boundary groups, 526–527
  - creating, 527–530
- branches
  - current, 499–500
    - LTSB (Long-Term Servicing Branch), 500–501
  - technical preview, 501
- Client Push Installation method
  - configuring, 530–531
  - excluding servers, 531
  - manual installation, 531
- client settings, 532–534
- collections, 535–536
  - uses, 535
- Computer Agent, 532
  - configuration, 517–518
    - Active Directory methods, 521–526
    - discovery methods, 518–521
- discovery methods
  - Active Directory Forest Discovery, 518
  - Active Directory Group Discovery, 519
  - Active Directory System Discovery, 518–519
  - Active Directory User Discovery, 518–519
  - Delta Discovery, 521
  - Heartbeat Discovery, 520–521
  - Network Discovery, 520
- disk space recommendations, 505
- hardware inventory cycle, 532
- hardware recommendations, 505
- primary site servers
  - Active Directory and, 508
    - ADK 1703, 509–510
    - configuration, 510–517
    - installation, 510–517
    - SCCM, 506–507
    - schema extension and, 508
    - WSUS, 509
- server, hardware requirements, 459
- site servers
  - CAS (central administration site), 501–502
    - primary, 502
    - installation, 505–517
    - secondary, 502
- site system roles
  - Application Catalog web service point, 503
  - Application Catalog website point, 503
  - certificate registration point, 503
  - cloud-based distribution point, 503
  - component provider, 502
  - configurations supported, 504
  - distribution point, 503
  - endpoint protection point, 503
  - enrollment point, 503
  - enrollment proxy point, 503
  - fallback status point, 503
  - management point, 503
  - reporting services point, 503
  - services connection point, 503
  - SMS provider, 502
  - software requirements, 503–504
  - software update point, 503
  - state migration point, 503
  - software inventory cycle, 533
  - upgrade path, 458
- System Center Operations Manager, 27
- System Center VMM (Virtual Machine Manager), 221
- system partitions, 8

T
- tables, objects, 61–62
- Task Manager, 29–30
- Task Scheduler, 25–27
- templates, certificate templates, 406–407
  - built-in, 407
  - compatibility, 407–409
  - cryptography, 411–412
  - issuance requirements, 415–416
  - properties, 410
  - publishing certificates, 409–410
  - request handling, 410–411
  - requestors, 416–417
  - security, 413–414
- Test-Cluster cmdlet, 143
- tokens
  - groups, 371–372
  - token bloat, 372
- Trojans, 287
- troubleshooting, Application and System logs, 28–29

U
- UAC (User Account Control), domain
  - controllers and, 363
- UEFI (Unified Extensible Firmware Interface), 4, 325
UMCI (user mode code integrity), 325  
unpause command, 269  
updates, cluster aware, 148–149  
upgrades  
cluster, rolling, 117  
clusters, 141–142  
user accounts  
Active Directory Users and Computers, 292–293  
Credential Guard, 296–297  
Group Policy, rights, 289–292  
PowerShell  
deleted, restoring, 370  
reports, 368–369  
stale, 369–370  
privileges, delegating, 295–296  
Protected Users groups, 294–295  
securing, 292–293  
security, 288  
privileged access, 289–292  
user management, AD DS, 366–368  
user-created variables, 83  

V  
Validation Wizard, 142–143  
Variable: drive, 84  
variables  
clearing, 84  
environment variables, 84–85  
PowerShell  
automatic, 83  
preference, 83  
user-created, 83  
removing, 84  
VHDX format, 120  
virtual hard disks  
differencing, 121  
dynamically expanding, 120  
fixed size, 120  
pass-through, 121  
recommendations, 121  
Virtual Machine Connection window,  
checkpoints, 125  
virtual machines, 2  
architecture, 260  
checkpoints, 125  
custering  
guest clustering, 132–133  
host clustering, 132  
configurations, 122–123  
containers comparison, 260  
entrypoint, 267  
exporting, 125–126  
Generation 2, 123  
guest operating systems, 116  
high-availability option, 132  
Hyper-V  
discrete devices, 124  
integration services, 124  
ew features, 117–118  
resource metering, 124  
secure boot, 124  
shielded, 123–124  
smart paging, 124  
Hyper-V Replica, 129–130  
importing, 125–126  
installation, 5  
live migration, 126, 127–128  
MAC address spoofing, 119  
migration, 126–127  
Exporting and Importing Virtual Machines, 127  
Live Migration, 127  
Quick Migration, 127  
Virtual Machine and Storage Machine, 127  
PowerShell Direct, 126  
shielded, 117  
states, 124  
virtual switches, 121–122  
Virtual Secure Mode, 325  
Virtual Secure Mode Protected Code Integrity, 325  
virtual switches, 121  
external, 122  
internal, 122  
private, 122  
virtualization. See also Hyper-V  
deployment and, 19–20  
licensing, 1, 2  
nested, 117, 119–120  
network adapter teaming, 183  
Sysprep, 12–13  
viruses, 287  
VM Monitor Mode, extensions, 118  
VMK (volume master key), 299  
VMM (Virtual Machine Manager), System Center, 20, 221  
compute fabric, 470  
configuration, 466–469  
Database Configuration screen, 467–468
library configuration, 468
port configuration, 468–469
service account, 467–468
DHCP (Dynamic Host Configuration Protocol), 470–471
DNS (Domain Name System), 470
host groups, 470
Hyper-V
clusters, 470
hosts, 470
infrastructure servers, 470–472
installation
Diagnostic and Usage Data, 467
Getting Started screen, 466
license agreement, 466
location, 467
prerequisites, 467
product registration, 466
library, 470
network fabric
logical, 472
creating, 473–474
virtualization gateways, 473
VM, 472
creating, 475–476
server, hardware requirements, 459
storage fabric
devices, 476–477
RAID, 476
SAS (Serial Attached SCSI), 476
upgrade path, 458
virtual machines
Create Virtual Machine Wizard, 479–480
destination, 480–481
hardware configuration, 480
provisioning, 478
VMware vCenter servers, 470
VMware vSphere hosts, 470
VMQ (virtual machine queue), 122
VMware, 2
[void] data type, 78
volume licensing, 3–4
VPN (virtual private network), 210
Always On VPN, 217–218
DirectAccess and, 211, 218
GRE (Generic Routing Encapsulation), 222
latency, 210
point-to-site, 222
protocols
IKEv2, 212
L2TP, 212
PPTP, 211
SSTP, 212
RADIUS, 217
server, configuration, 213–215
site-to-site, 222

W
WAP (Web Application Proxy), 211, 218–219
WDS (Windows Deployment Services)
image types, 16
installation, 16–19
web services, PKI (public key infrastructure) and, 392
-WhatIf parameter, 53–54
while loop, 102–104
wildcards, 76–77
filters and, 207
Windows Defender
disabling, 322
domain controllers and, 363
scan options, 322
Windows Firewall, 179, 185
domain controllers and, 363
enabling, 186
profiles
Domain, 186
Private, 186
Public, 187
rules, inbound, 187
Windows Firewall with Advanced Security, 300–302
firewall profiles, 300
inbound rules, 302–303
outbound rules, 302–303
PowerShell, cmdlets, 303
Windows Server 2012
Active Directory Recycle Bin, 340
DAC (Dynamic Access Control), 340
Fine-Grained Password Policies, 340
virtualization, 340
Windows Server 2012 R2, AD DS
Conditional Access, 340
Multifactor Authentication, 340
Workplace Join, 340
Windows Server 2016
activation, 10–11
editions, 1–2
differences, 1–2
Hyper-V Containers, 2
Shielded Virtual Machines, 1
Software Defined Networking, 2
Storage Replica, 2
Storage Spaces Direct, 2
Virtualization Licensing, 1
Windows Server 2016 Datacenter, Standard comparison, 1–2
Windows Server 2016 Essentials, 4
Windows Server 2016 Standard Datacenter comparison, 1–2
with Hyper-V, 2
Windows Server Backup, 21
Windows Storage Server 2016, 4
Work Folders
deployment
hosted, 253

multiple-site, 253
preparation, 252–253
single-site, 253
Server Manager installation, 253
workgroups, WORKGROUP, 179
Workplace Join, 340
WS-Federation, 423
WSUS (Windows Server Update Server), 196–197

X
XenServer, 2
[xml] data type, 78
XML files, credentials, 71–73