# Index

**A**

AAS (application assignment scripts), Windows Installer, 216
access protection
AD FS. *See* AD FS (Active Directory Federation Services)
AD RMS. *See* AD RMS (Active Directory Rights Management Services)
WAP. *See* WAP (Web Application Proxy)
ACEs (access control entries), 52, 81
ACLs (access control lists), 52, 81
Active Directory
configuring DNS integration with, 35–37
features, 45–46
new to, 14–15
overview of, 44–45
security principals, 46–47
troubleshooting replication, 130–131
Active Directory Administrative Center tool, 27, 83, 90–94
Active Directory Administrative tools, 27–28, 127
Active Directory Certificate Services (AD CS). *See also* certificates, 45
Active Directory Claims Provider Trusts Wizard, 288–289
Active Directory data store
backing up, 157, 160
must reside on NTFS partition, 5
performing authoritative restore, 165
restoring Active Directory, 164–165
restoring System State data, 162
supporting multimaster replication, 109
Active Directory Database Mounting tool, 28, 168–169
Active Directory delegation, 198
Active Directory Domain Services. *See* AD DS (Active Directory Domain Services)
Active Directory Domains and Trusts tool
assigning single-master operations, 147
defined, 27
managing multiple domains, 144–145
managing trust relationships, 152–153
Active Directory Federation Services. *See* AD FS (Active Directory Federation Services)
Active Directory Installation Wizard
adding additional domain controllers, 142–144
configuring DNS automatically, 17, 36
creating domain trees and forests, 172
promoting server to domain controller, 139–140
Active Directory Lightweight Directory Services (AD LDS), 13, 28, 170
Active Directory Migration Tool (ADMT), 51, 70
Active Directory Module for Windows PowerShell tool, 28
Active Directory objects
configuring user principal name, 67
creating with Active Directory Migration Tool, 70
creating with Active Directory Users and Computers, 65–67
Group Policy settings for types of, 182–183
importing objects from file, 69
linking existing GPOs to, 191
managing replication using, 112–113
offline domain join of computer, 70
organizational sections, 63–64
OU as logical group of, 47
publishing, 86–89
querying/finding, 89–90
types of, 64–65
Active Directory objects – AD FS (Active Directory Federation Services)

using Active Directory Administrative Center, 90–94
using templates, 67–69
Active Directory objects, managing
filtering and advanced features, 76–77
groups, 74–76
moving, deleting and renaming, 77–78
properties, 70–73
resetting existing computer account, 79
security and permissions, 80–82
using Dynamic Access Control, 79–80
Active Directory Recycle Bin, 78, 166
Active Directory replication
Active Directory objects managing, 112–113
keeping replicas up-to-date, 32
managing traffic using sites, 109
monitoring, 129–132, 169–170
overview of, 107
reducing traffic using multiple domains, 133
troubleshooting, 129–132
using DFSR, 111–112
Active Directory replication, configuring
bridgehead servers, 124
connection objects, 122
DNS SRV records, 129
domain controller cloning, 128–129
intersite replication, 118–120
intrasite replication, 118
moving server objects between sites, 122–123
overview of, 117–118
RDOCs and replication, 124–125
server topology, 125–127
site links/site link bridges, 120–122
Universal Group Membership Caching, 128
Active Directory Service Interfaces Editor (ADSI Edit), 31, 84–86, 170
Active Directory sites
as Active Directory replication objects, 112–113
concepts of, 107–108
configuring, 116–117
creating, 113–115
defined, 108
Distributed File System Replication, 111–112
implementing subnets, 112–117
managing replication traffic, 109, 111
planning, 109–111
service requests, 108
Active Directory Sites and Services tool
creating sites, 113–115
creating subnets, 115–116
defined, 28
intersite replication, 119
moving servers between sites, 125–127
Active Directory Users and Computers tool, 28
AD CS (Active Directory Certificate Services). See also certificates, 45
AD CS Configuration Wizard, 255–256
AD DS (Active Directory Domain Services)
Active Directory feature, 45
AD RMS requirements, 295
certificate authority name, 257
installing on server core using PowerShell, 21–22
AD FS (Active Directory Federation Services)
AD RMS integration with, 294
attribute stores, 277
certificates, 284–285
claim descriptions, 277
claim pass-through/transformation rules, 288–290
claim rules, 277
claims, 274–275
claims provider, 275
claims provider/transform claims rules, 286
configuring, 282–284
enabling compound authentication, 290–291
endpoints, 276–277
AD RMS server, AD RMS, 294
AD RMS service account, AD RMS, 294
Add Roles And Features Wizard
backing up Active Directory, 163–164
creating new subdomain, 140–141
creating RODC server, 22–23
installing AD Certificate Services,
252–253
installing AD Federation Services role,
280–281
installing AD Rights Management
Services role, 296–297
administration
delegation of. See delegation of
administrative control
drawbacks of multiple domains, 135
using multiple domains to decentralize,
134
administration, Active Directory
applying group policies, 53
cmand prompt for configuration,
94–95
creating Active Directory objects, 63–70
exam essentials, 97–98
exam objectives, 43
group policies for security, 82–86
managing objects. See Active Directory
objects, managing
organizing objects with OUs. See OUs
(organizational units), Active
Directory
overview of, 44
PowerShell commands, 95–97
publishing objects, 86–89
querying Active Directory, 89–90
review Q & A, 99–101, 317
security principals, 46–47
summary, 97
understanding features, 45–46
using Active Directory Administrative
Center, 90–94
Administrative Center tool, Active Directory,
27, 85, 90–94
Administrative Templates, Group Policy settings, 183
Administrative tools, Active Directory, 27–28, 127
ADMT (Active Directory Migration Tool), 51, 70
ADMX Central Store, Group Policy settings, 183
Adprep /domainprep, 15
Adprep /forestprep, 15
Adprep, installing Active Directory, 15–16
Adprep /rodcprep, 15
ADSI Edit (Active Directory Service Interfaces Editor), 31, 84–86, 170
Advanced Features, Active Directory objects, 75–76
advertising, Windows Installer support for, 215–216
AGDLP (or AGLP), group strategy, 75
AGL (AGDLP), group strategy, 75
AGUDL (AGUDL), group strategy, 75
anonymous authentication, 259
application assignment scripts (AAS), 216
application data partitions
creating, 31–32
managing replicas, 32
managing using ntdsutil, 33–35
overview of, 30–31
removing replicas, 33
Application log, Event Viewer information
on, 26–27
applications
compatibility, ReFS, 4
deploying, 217–218
publishing Web Application Proxy, 306
AppLocker, 220
archive attributes, viewing folder, 158–159
assigning applications, 217–218, 220–222
attribute stores, AD FS, 277
attributes
defined, 15
digital certificate, 203
viewing system file, 158–159
Auditors role, AD RMS, 296
Auditpol.exe utility, creating GPO, 189
audits
with AD Domain Services, 45
CA policy, 264
Dynamic Access Control for, 80
logging events to Security log via, 52
security, 45
using security, 46
AULP (AGUDLP), group strategy, 75
authentication
AD Federation Services, 291, 308
certificate-based, 259
compound, 290–291
with gMSAs, 46
Kerberos. See Kerberos authentication
managing trust relationships, 152
troubleshooting replication, 131
Universal Group Membership Caching, 128
Web Application Proxy preauthentication, 307–308
Authoritative Restore, 164–165
authorization claims, AD FS, 287–289
auto-enrollment
configuring in Group Policy, 204–205
GPO certificate, 257–258
automated installations, Windows Installer, 215
availability, Resilient File System, 3
Azure AD Join, 15

Backup utility, Windows Server 2016, 158
backups, Active Directory
AD Rights Management Services, 301–302
Bare Metal Restore and, 161–162
certificate authority server, 264–265
configuring with wbadmn, 170–171
reasons for, 157–158
restoring Active Directory, 164–167
restoring GPOs, 163
restoring System State data, 162
scheduling, 162
setting up, 163–164
System State data, 160–161
types of, 158–160
Windows Server 2016 Backup utility, 158
backups, GPO, 208–209
bandwidth, network
as constraint, 105–106
intersite replication optimized for low,
118–120
UGMC reducing, 155
Base CRLs (certification revocation lists), 251
batch file commands, 199
batch files, 94–95
Block Policy Inheritance option, Group
Policy, 187
BMR (Bare Metal Restore), 161–162
boot files, System State backup for, 160
bridgehead servers
configuring replication, 124
planning your sites, 110
topology, 110–111
browsing network, testing connectivity, 9
Built-in container, Active Directory
organization, 63–64
business needs
mapping OU structure to, 50
using multiple domains for, 133–134
BYOD (bring your own device), WorkPlace
Join, 292–293

C
CA hierarchy, planning
certificate validation, 251
terprise CAs, 248–250
implementing cryptographic options,
246–248
online responders, 252
overview of, 246
private key, 248
validity periods, 250–251
CAs (certificate authorities)
as AD Certificate Services role, 245
defined, 203
displaying current site name for, 263
naming, 256–257
policy auditing, 264
policy servers, 250
using hash algorithms to sign CA
certificates, 256
categories, setting application, 226–227
CDPs (CRL distribution points), 251
CEP (Certificate Enrollment Policy Web
Server), 246
Certificate Authority Role Service, 245
certificate-based authentication, 259
Certificate Enrollment Web Services (CES),
244–246, 258–259
certificate publishers, 203
Certificate Services. See AD CS (Active
Directory Certificate Services)
certificate templates, 204, 260–264
Certificate Templates Management console,
261–262
certificates
AD Certificate Services, configuration,
255–256
AD Certificate Services, features, 244–245
AD Certificate Services, installation,
252–255
AD Certificate Services, PowerShell for,
266–267
AD Certificate Services, roles, 245–246
AD Federation Services, 284–285,
292–293
backing up certificate authority server,
264–265
CA names, 256–257
certificate templates, 260–264
configuring automatic enrollment in
Group Policy, 204–205
configuring/Managing key archive/
recovery, 263–266
cryptographic options, 246–248
CSP/KSP ordering, 259–260
enforcing certificate renewal with same key, 259
enterprise CAs, 248–250
exam essentials, 268
domain structure, 7–8
exam objectives, 243
Group Policy certificate auto-enrollment, 257–258
key-based renewal for non-domain-joined computers, 258–259
Copyright, 2018. All rights reserved.
Cygnus, 750
Cygnus, 61
326
Claim descriptions, AD FS, 277–280
claim pass-through/transformation rules, 288–290
claim transformation claim rules, 288–289
claim types. See claim descriptions, AD FS
claims, AD FS
attribute stores, 277
claim descriptions, 277
claims provider, 275
endpoints, 276–277
identity solution based on, 274–275
new model for, 279–280
relying party, 275–276
rules, 277
claims-aware agent, AD FS role, 278
claims provider, AD FS, 275, 286, 288–289
claims rules, 288–289
client
forcing GPO to update from, 192–193
verifying network connectivity, 7–8
client-side extensions (CSEs), group policies, 185
cloning, domain controller, 128–129
cluster key password, AD RMS, 295, 301
cluster key storage location, AD RMS, 295
cluster name, AD RMS, 295
COM+ Class Registration database, System
State backup, 160
comma-separated value files, importing objects from, 69
certificate
command prompt, Active Directory configuration, 94–95
certificate template, 260–261
compound authentication, AD FS, 290–291
corruption, intersite replication with, 119
certificate
computer account managing, 28
migrating, 70
offline domain join of, 70
resetting existing, 79
as security principal, 46–47

Computer Management, 6–7
certificate
computer name (NetBIOS name), planning domain structure, 13
certificate
computer name (or NetBIOS name), planning domain structure, 13
Computer objects
defined, 64–65
Group Policy settings, 182–183
properties, 72
Security Settings section of GPO, 184–185

Computers container, Active Directory organization, 64
connection objects, configuring replication, 122

connectivity
Active Directory using replication for, 107
verifying Active Directory via client, 29
verifying network, 7–10

constraints, network, 105–106
Contact objects, 65
copy backups, 159
copying GPOs, 209–210
corrupted applications, Windows Installer repairing, 215
cost
creating site links/site link bridges for replication, 120
as network constraint, 106
CRL distribution points (CDPs), 251
CRLs (certification revocation lists)
CA responsible for publishing, 246
certificate validation and, 251
using OCSP online responder, 252
cross-forest trusts, 150
cryptographic mode, AD RMS requirement, 294
cryptography options, CAs, 246–248
CSEs (client-side extensions), group policies, 185
CSP/KSP (cryptographic service provider/key service provider) ordering, 259–260
CSPs (cryptographic service providers), 246–248
csvde.exe utility, importing objects from file, 69
default GPO, resetting, 210–211
default packages, software installation settings, 225–226
default SID filtering, on external trusts, 150
defunct schema classes and attributes, forests, 12
delegation
Active Directory, 197
as computer object property, 72
Kerberos constrained. See KCD (Kerberos constrained delegation)
overview of, 51
responsibilities and, 62
understanding rights and, 52
delegation of administrative control
defined, 52, 63
GPOs, 197–198
OUs, 51–53, 59–62
troubleshooting OUs, 63
Delegation of Control Wizard, 59–62, 98
deleting
Active Directory objects, 78
backups for accidental, 157
backups for malicious, 157
OUs, 57–58
protecting OUs from accidental, 54, 78
restoring with Active Directory Recycle Bin, 166
vs. disabling user accounts, 47, 73
Delta CRLs (certification revocation lists), 251
demotion, domain controller, 33, 143–144
Deny permissions, ACLs, 81
dependency changes, 279
deployment
of Active Directory in Windows Azure, 24
application, 217–218
software. See software deployment, through GPO
deprovisioning, Active Directory objects, 73
Device Registration Service (DRS), WorkPlace Join, 292–293
DFSR (Distributed File System Replication), 111–112
DAC (Dynamic Access Control), 79–80
DACL (Discretionary Access Control List), 210
daily backups, 160
data
backups. See backups, Active Directory integrity, 4
store. See Active Directory data store
database
Active Directory Database Mounting tool, 28, 168–169
backing up AD Rights Management Services, 301–302
requirement for AD Rights Management Services, 294
DCGPOFix utility, resetting default GPO, 210–211
decentralized administration, multiple domains for, 134
Demystifying
KCD (Kerberos constrained delegation)
overview of, 51
responsibilities and, 62
understanding rights and, 52
deployment
of Active Directory in Windows Azure, 24
application, 217–218
software. See software deployment, through GPO
deprovisioning, Active Directory objects, 73
Device Registration Service (DRS), WorkPlace Join, 292–293
DFSR (Distributed File System Replication), 111–112
D}
differential backups, 160
directory services, Event Viewer, 26
Directory Services Restore Mode (DSRM), 162
Disable, vs. Delete user accounts, 47, 73
Disabled setting, Group Policy items, 181–182
disaster recovery (DR), 142–143
disaster recovery plan (DRP), 142–143
Discretionary Access Control List (DACL), 210
Disk Management, 6–7
disks
NTFS quotas, 4
Resilient File System updating, 4
types of Windows Azure VM, 24
Distributed File System Replication (DFSR), 111–112
distribution groups, 46, 75
DLLs (dynamic link libraries), 214
DNS
configuring integration with Active Directory, 35–37
Event Viewer information on, 26
installing during Active Directory installation, 14
planning domain structure, 13–14
Service (SRV) records, 129
using multiple domains for multiple, 134
domain controllers
cloning, 128–129
configuring server topology, 125–126
controlling with AD Domain Services, 45
converting servers to, 16–17
creating additional, 142–143
demoting, 143–144
installing additional with IFM, 24–25
multiple domains reducing replication traffic, 133
planning for placement of, 143–144
promoting, 17–21, 139–140
replication between, 107, 110
using single tree, 136–137
Domain Controllers OU, Active Directory organization, 64
domain functional levels, 10–11
domain local groups, 75
domain names, multiple domains for multiple, 134
Domain Naming Master, 145
domain operations masters, 145–146
Domain Services. See AD DS (Active Directory Domain Services)
domain trees and forests
adding additional domain controllers, 142–143
creating domain tree, 140
creating new subdomain, 140–141
joining new domain tree to forest, 142
overview of, 135
planning, 136
promotion process, 139–140
upgrading existing, 156
using forests, 138–139
using single tree, 136–137
domains. See also Active Directory Domains and Trusts tool
Active Directory Module for Windows PowerShell managing, 28
adding first Windows Server 2016 DC to existing, 15
drawbacks of multiple, 135
joining computer to Active Directory, 29–30
planning structure for Active Directory installation, 13–14
potential relationships between sites and, 108
reasons for using multiple, 132–134
removing trusts between, 150
renaming, using forest functionality, 12
Domains level, GPO processing, 186
DR (disaster recovery), 142–143
DRP (disaster recovery plan), 142–143
DRS (Device Registration Service), WorkPlace Join, 292–293
Dsamain.exe, 168–169
DSRM (Directory Services Restore Mode), 162
Dynamic Access Control (DAC), 79–80
dynamic link libraries (DLLs), 214
dynamic volumes, NTFS, 4

E

Elevated privileges, Windows Installer, 214–215, 229
Elevation-of-privileges attack, 150
Email
   distribution groups, 46
   sending/receiving with SMTP, 118
Enabled setting, Group Policy, 181–182
   encryption, NTFS, 4
Endpoints, AD FS security modes, 276–277
Enforced (No override) option, Group Policy, 187, 198–199
Enrollment
   AD Certificate Services, 244–245
   AD Rights Management Services, 294
Enterprise CAs, 248–250
Event logs, troubleshooting replication, 130
Event Viewer, 25–27
Export
   AD RMS templates, 300
   data from AD with ldifde/csvde.exe, 69, 94–95
   private keys, 265
   starter GPOs, 184
   trusted publishing domain, 304–305
   trusted user domain, 304
External trusts, 150

F

Failover clusters, DFSR, 111
FAT/FAT32, converting to NTFS, 6
Fault tolerance, 107, 142
Federated identity management, forests, 13
Federated Trust, AD RMS trust policies, 303
Federation Metadata fields, relying-party trust, 285–286
Federation Service Proxy, AD FS role service, 278
Federation Services. See AD FS (Active Directory Federation Services)
   fields, user template, 67–69
   file extension mappings, software installation settings, 226–227
   file system encryption, NTFS, 4
   file system verification
      NTFS, 4–6
      overview of, 2–3
      Resilient File System, 3–4
      viewing disk configuration, 6–7
Files
   Bare Metal Recovery option, 161–162
   importing objects from, 69
   Windows Installer, 216–217
   Windows Installer preventing conflicts between, 215
Filtering
   Active Directory object options, 75
   Group Policy security, 195–199
Find dialog box, Active Directory, 89–90
Fine-grained password policies, 84–86, 91–92
Firewalls, troubleshooting replication, 130
Flexibility, decreased by multiple domains, 135
Folder redirection, Group Policy settings, 205–206
Force Policy Inheritance option, Group Policy, 187
Foreign security principals, Active Directory organization, 64
Forest operations masters, 145
Forest-wide authentication, 150
Forests. See also domain trees and forests about, 12–13
   default trusts, 149
   trusts, 12
Formats, log files saved in Event Viewer, 27
FQDN (fully qualified domain name)
- defined, 134
- not using for CA common name, 257
- AS RMS cluster name requirement, 295

G

GC (global catalog) servers
- configuring server topology, 126–127
- demoting domain controllers, 143
- managing multiple domains, 153–155
- replication enhancements, 12
- using Universal Group Membership Caching, 126–127
- global groups, 75, 85–86
- gMSAs (group Managed Service Accounts), 45–46

GPMC (Group Policy Management Console)
- backing up/restoring GPOs, 163, 208–209
- creating GPOs, 189–190
- delegating administrative control of GPOs, 197
- forcing GPO to update, 192
- importing/copying GPOs, 209
- item-level targeting setup, 208
- linking existing GPOs to Active Directory, 191
- managing GPOs with PowerShell, 206
- opening Migration Table Editor, 210
- publishing/assigning applications, 221
- using Group Policy Infrastructure Status Dashboard, 236

GPOs (Group Policy objects)
- about Group Policy, 180–185
- backing up and restoring, 163, 208–209
- certificate auto-enrollment, 203–205, 257–258
- creating, 188–191
- creating for each OU, 48
- defined, 48
- delegating administrative control, 197–198
- exam essentials, 237–238
- exam objectives, 179
- forcing to update, 191–193
- group policies in, 185–186
- importing/copying, 209
- inheritance, 186–187
- inheritance/filtering, 198–199
- item-level targeting, 207–208
- linking to Active Directory, 191
- Loopback Policy, 201
- migration tables, 209–210
- network configuration, 201–203
- network settings, 203
- overview of, 180
- planning strategy, 187–188
- PowerShell Group Policy cmdlets, 206–207
- redirecting folders, 205–206
- resetting default, 210–211
- review Q & A, 239–241, 318–319
- script policies, 199–201
- security and, 82–84
- security filtering, 195–196
- software deployment. See software deployment, through GPO
- summary, 236–237
- troubleshooting, 229–236
- understanding, 185–186

GPPs (Group Policy preferences), 183
- gpresult.exe utility, 230, 234–235
- GPUpdate.exe command, 193–194
- graphical deployment, AD FS role, 282–283
- group Managed Service Accounts (gMSAs), 45–46

Group objects, 65
- group policies, 53, 185

Group Policy
- general settings, 181–184
- introducing, 180–181
- Restricted Groups, 185
- security and permissions, 80–81
- security settings, 82–84, 184–185
- Software Restriction Policy, 185
Group Policy Infrastructure Dashboard, 236
Group Policy Management Console tool, 84, 208–210, 220, 222–223
Group Policy Results Wizard, 231–233
Group Policy Slow Link Detection, software deployment, 220
group scope, 75
groups
  assigning users to, 48
  creating, 76
  creating strategies, 75
  managing security and permissions, 80–82
  migrating, 70
  placing in OUs, 48
  as security principal, 46
  setting up properties, 74–75
types of, 74–75
understanding, 74

IFM (install from media), additional DCs, 24–25
importing
  GPOs, 209
  objects from file, 67–69
-IncLuMeManaGementToOlS cmdlet, 254
incremental backups, 159–160
InetOrgPerson objects, 65
information protection
  AD Federation Services. See AD FS (Active Directory Federation Services)
  AD Rights Management Services. See AD RMS (Active Directory Rights Management Services)
  WAP. See WAP (Web Application Proxy)
Infrastructure as a Service (IaaS), deploying
  AD in Windows Azure, 24
Infrastructure Master, 146
inheritance
  Group Policy, 186–187, 198–199
  OU, 51–53, 63
initialization files, Windows Installer, 216
install from media (IFM), additional DCs, 24–25
Install-WinDoWsFeatuRe cmdlet, 254–255
installation
  AD Certificate Services, 252–255
  AD Federation Services, 278–281
  AD Rights Management Services, 296–298
  remote Windows, 46
software. See software deployment, through GPO
Installer program, Windows Installer, 213
Installer service, Windows Installer, 213
installing Active Directory
  about domain functional level, 10–11
  about forest functionality, 12–13
  additional domain controllers, 24–25
  application data partitions, 30–35
  deploying Active Directory in Windows Azure, 24
exam essentials, 37–38

Hacks, 90 percent are internal network, 44
hardware, 155, 157
hash algorithms, 247, 256
hidden shares, software deployment, 219
hierarchy
certification authority, 246–252
Group Policy settings, 186
multiple domains for levels of, 134
naming OUs, 51
parent-child relationships and OU, 52–53
historical information, backups of, 157
HTTP.SYS, AD FS, 278, 279

IaaS (Infrastructure as a Service), deploying
  AD in Windows Azure, 24
IDNs (Internationalized Domain Names), AD Certificate Services, 245
exam objectives, 1
installation process, 16–23
new to Active Directory, 14–15
overview of, 2
planning domain structure, 13–14
prerequisites, 16
read-only domain controllers, 15
review Q & A, 39–41, 316
summary, 37
using Adprep, 15–16
verifying file system, 2–7
verifying installation, 25–30
verifying network connectivity, 7–10
Internationalized Domain Names (IDNs), AD Certificate Services, 245
Internet, 10, 105
Internet Explorer, and AD RMS, 295
intersite replication, 117–122
IP addresses, not supported on Windows Azure VMs, 24
ipconfig utility, viewing TCP/IP information, 8
item-level targeting, managing GPOs, 207–208

K
KCC (Knowledge Consistency Checker), 32, 120
KCD (Kerberos constrained delegation), 45
Kerberos authentication
  as Active Directory feature, 45
AD Federation Services and, 289, 290–291
  in automatic certificate renewal, 259
key archive, recovery and, 265–266
key length, cryptographic options, 247
Key Recovery Agent template, 265–266
KSPs (key storage providers), 246–248

L
LANs (local area networks), 105
LDAP (Lightweight Directory Access Protocol), 13, 31
ldifde.exe utility, 69
LDP tool (ldp.exe), 31
legality, multiple domains for, 134
life cycle, software management, 211–213
line-delimited files, importing from, 69
linked value replication, 12, 109
links, existing GPO to Active Directory, 191, 194
Local Computer Policy Tool, creating GPOs, 188–189
Local level, GPO processing, 186
location, application data partition, 32
log files, Event Viewer, 26–27
logging mode, RSoP, 230, 231–233
logical components, Active Directory sites, 108
logical grouping of resources, OU structure, 49–50
logon times, UGMC, 155
Loopback Policy, GPOs, 201

M
maintaining Active Directory
  Active Directory replication and sites, 106–112
  backups, 157–164
demotion domain controller, 143–144
domain trees and forests. See domain trees and forests
exam essentials, 172–174
exam objectives, 103
implementing sites and subnets, 112–117
managing multiple domains. See multiple domains, managing
monitoring/troubleshooting replication, 129–132
network planning overview, 104–106
offline maintenance, 167–171
overview of, 104
reasons for creating multiple domains, 132–135
replication. See Active Directory replication, configuring
restoring, 164–167
review Q & A, 175–177, 317–318
summary, 171–172
maintenance
offline, 167–171
software, 212
Managed Service Accounts, 45, 64
management
AD RMS SCP, 298
drawbacks of multiple domains, 135
GPO, 193–194
OU, 57–62
mandatory upgrades, software, 223
mapping
business needs to OU structure, 50
troubleshooting organizational issues, 63
Microsoft Federation Gateway, 303
Microsoft Passport, 15
Microsoft Transformation (MST) files, Windows Installer, 216
Microsoft Windows Installer. See Windows Installer
migration, AD Migration Tool, 51, 70
Migration Table Editor, 210
migration tables, 209
MIM (Microsoft Identity Manager), access with PAM, 15
Minimal Server Interface, AD Certificate Services, 244
MMC (Microsoft Management Console), 27
monitoring, Active Directory replication, 129–130
mounted drives, NTFS, 4–5
moving
Active Directory objects, 78
OUs, 57–58
servers between sites, 125–127
MSI (Microsoft Windows Installer). See Windows Installer
MSMQ Queue Alias objects, 65
MST (Microsoft Transformation) files, Windows Installer, 216
multifactor access control mechanism, AD FS, 291–292
multifactor authentication, 291–292
multimaster replication, 109, 111–112, 145
multiple domains, managing
global catalog servers, 153–155
Name Suffix Routing, 153
overview of, 144
single-master operations, 145–148
trusts, 149–152
Universal Group Membership Caching, 155
upgrading existing domains and forests, 156
UPN suffixes, 153
multiple domains, reasons for using, 132–135

N

Name Suffix Routing, multiple domains, 153
naming conventions
certificate authorities, 256–257
OUs, 50–51
NDES (Network Device Enrollment Service), AD Certificate Services, 246
NetBIOS name (computer name), planning
domain structure, 13
network connectivity
deploying Active Directory IaaS, 24
troubleshooting replication, 130
verifying Active Directory installation, 7–10
Network Device Enrollment Service (NDES), AD Certificate Services role, 246
network location, backups to, 159
Network Time Protocol (NTP), Windows Time service, 146
  networks
    configuring settings, 203
    constraints, 105–106
    managing Group Policy configuration, 201–203
    types of, 105
  nonauthoritative restore, 165
  nonmandatory upgrades, software, 223
  normal backups, 159
  Not Configured setting, Group Policy items, 181–182
  NTDS Site Settings, intersite replication, 119
  ntdsutil utility
    application data partitions, 33–35
    definition of, 31
    offline defragmentation, 169
    offline maintenance, 167–168
  NTFS, 4–6
  NTP (Network Time Protocol), Windows Time service, 146

O

objects. See Active Directory objects
OCSP (Online Certificate Status Protocol), 245, 252
offline defragmentation, 169
offline domain join, computer accounts, 70
offline files and folders, 202, 206
offline maintenance
  Active Directory Database Mounting tool, 168–169
  ADSI Editor, 170
  monitoring replication, 169–170
  ntdsutil utility, 167–168
  offline defragmentation, 169
  wbadmin commands, 170–171
offline stand-alone root CAs, 249, 250
on-demand installations, Windows Installer, 215
one-way trusts, 149

Online Certificate Status Protocol (OCSP), 245, 252
online responders, certificate requests, 252
operations masters, 145
organizational issues, troubleshooting
  OUs, 63
  OU level, GPO processing, 186
  OU objects, 65
  OUs (organizational units), Active Directory
    administering properties, 58–59
    benefits of, 48–49
    creating, 53–57
    delegating administrative control, 51–53
    group policies, 53
    inheritance, 51
    moving, deleting and renaming, 57–58
    naming conventions, 50–51
    not functioning as security principals, 46–48
    overview of, 47–48
    planning structure for, 49–51
    purpose of, 48
    security and permissions, 80–81
    troubleshooting, 62–63
    viewing GPO links to, 194

P

package defaults, software installation
  settings, 225–226
package file, Windows Installer, 216–217
PAM (privileged access management), 14–15
parent-child relationships, OU hierarchy,
  52–53
partitions, NTFS, 5–6
pass-through claim rules, 288–289
pass-through preauthentication, WAP, 307–308
Password Replication Policy (PRP), RDOCs, 125
Password Settings objects (PSOs), 84–86, 91–92
passwords, automatic certificate renewal, 259
passwords, fine-grained policies, 84–86, 91–92
patches, 212, 216
PDC Emulator Master, 146
performance
adding domain controllers for, 142–143
network cost and, 106
permissions
deleing control of OUs, 51–53, 59–62
managing security and, 80–82
security filtering of GPOs, 195–197
personnel, network cost and, 106
physical components, Active Directory sites, 108, 112–117
ping command, testing network connectivity, 9
PKI (public key infrastructure). See also certificates
AD Certificate Services managing, 45
certificate validation/revocation, 251
defined, 203
multiple, 250
PKI-savvy applications, defined, 204
planning
backups, 161
CA hierarchy, 246–252
domain controller placement, 143–144
domain structure, 13–14
Group Policy strategy, 187–188
network, 104–106
OU structure, 49–51
trees and forests, 136
your sites, 109
planning mode, RSoP, 230, 233–234
policies
AD RMS trust, 302–303
CA auditing of, 264
for each OU, 48
PowerShell
Active Directory and, 95–97
Active Directory Module for, 28
AD FS/Web Application Proxy commands, 308
deploying AD FS, 283–284
forcing GPOs to update from, 192
installing AD CS, 21–22, 253–255
installing AD FS, 281
maintaining AD CS, 266–267
managing GPOs with Group Policy, 206–207
seizing roles, 147–148
testing network configuration, 8–10
preauthentication, Web Application Proxy, 307–308
preferences, Group Policy, 183
Printer objects, 65
printers, publishing, 87–88
private keys, 248
privileged access management (PAM), 14–15
privileges, Windows Installer elevated, 214–215, 229
Programs and Features icon, 218
promotion
creating domain trees and forests, 139–140
domain controllers in AD installation, 17–21
drawbacks of multiple domains, 135
properties
Active Directory objects, 70–73
group, 74–75
OU, 58–59
system file attributes, 158–159
Windows Installer package file, 216–217
Protect Container From Accidental Deletion for all OUs, 54, 78
PRP (Password Replication Policy), RDOCs, 125
PSOs (Password Settings objects), 84–86, 91–92
publication intervals, CRL, 251
publishing
Active Directory objects, 86–89
applications, 218
applications using Group Policy, 220–222
applications using Web Application Proxy, 306
certificate templates, 262
defined, 87, 306

querying, Active Directory, 89–90

RAID (Redundant Array of Independent Disks), NTFS, 4
RDC protocol, DFSR, 111
RDOCs (read-only domain controllers), replication, 124–125
realm trusts, 150
recovery
additional domain controllers for, 142–143
backups and. See backups, Active Directory
Bare Metal Recovery, 161–162
configuring key archive and, 265–266
configuring with wbadmin, 171
Dsamain.exe tool helping, 169
Recycle Bin, Active Directory, 78, 166
Redundant Array of Independent Disks (RAID), NTFS, 4
ReFS (Resilient File System), AD deployment, 3–4
Registry, System State backup for, 160
Relative ID (RID) Master, 145–146
reliability, additional domain controllers for, 142
relying party, AD FS, 275–276, 288–289
relying-party trust, AD FS, 285–286
Remote Procedure Call (RPC) protocol, 118, 245
remote storage, NTFS, 5
removable media
backups to, 159
setting Windows Installer to disallow, 229
removal, software, 214, 228–229
Rename
Active Directory objects, 78
OUs, 57–58
renewal, AD Certificate Services, 245
Repladmin utility, replication, 131–132, 169–170
replicas, application data partition, 32
replication. See Active Directory replication requirements
AD installation, 16
AD RMS, 294–296
resetting default GPO, 210–211
Resilient File System (ReFS), AD deployment, 3–4
resources, planning OU structure, 49–50
Restartable Active Directory Services, 166–167
restoring
Active Directory, 164–165
GPOs, 209
System State data, 164–165
using Active Directory Recycle Bin, 166
Restricted Groups setting, Group Policy, 185
Resultant Set of Policy (RSoP), 230–234
revocation, certificate, 263
revocation checking, PKI, 251
RID (Relative ID) Master, 145–146
Rights Management Services. See AD RMS (Active Directory Rights Management Services)
rights policy templates, distributed/archived, 305–306
RODCs (read-only domain controllers), 15, 21–22
roles
AD Certificate Services, 245–246
AD FS server, 277–278
AD RMS administrative, 294, 296
assigning single-master, 146–147
seizing single-master, 147–148
rollback, Windows Installer setting to prohibit, 229
root CAs (or root authority), 248–250
root domain
establishing domain tree, 136–137
establishing forest, 139
joining new domain tree to forest, 142
routers
network cost and, 106
troubleshooting replication, 130
RPC over IP, Intersite replication, 118
RPC (Remote Procedure Call) protocol, 118, 245
RSoP (Resultant Set of Policy), 230–234
rules, AD Federation Services, 277
Run The AD FS Management, 282–283

Kerberos and KCD authentication, 45
managing permissions and, 80–82
most hacks are on internal networks, 44
security principals as basis of Active Directory, 46–47
security groups
filtering GPOs, 195–197
properties for, 74–75
as security principal, 46
Security log, 26, 52
security principals, 46–47, 64
Security Settings dialog box, GPOs, 195–197
Security Settings section, GPOs, 184–185
security templates, Group Policy, 184
selective authentication, 150, 152
self-healing NTFS, 5
Server Core, AD Certificate Services, 244
Server Manager
configuring AD Certificate Services, 255–256
configuring AD Federation Services, 282–283
installing AD Certificate Services, 252–255
installing AD Federation Services role, 280–281
installing AD Rights Management Services, 296–298
publishing certificate templates, 262
server name indication (SNI), Web proxy service, 279
servers
backing up certificate authority, 264–265
configuring topology, 125–127
converting to domain controllers, 16–17
creating bridgehead server from, 124
forcing GPO to update from, 192
moving between sites, 122–123
service communications certificate, AD Federation Services, 285–286
service connection points (SCPs), AD RMS, 298

SAML authentication, AD Federation Services, 279–280
scalability, 3, 132–133
SChannel SSP (TLS/SSL), 46
schedules, 120, 162
Schema Master, 145
schema, of domains within forest, 139
SCPs (service connection points), AD RMS, 298
script policies, managing GPOs, 199
searches, in Windows Installer, 229
security
AD Rights Management Services. See AD RMS (Active Directory Rights Management Services)
auditing, 46
filtering GPOs, 195–197
fine-grained password policies, 84–86
Group Policy settings, 82–84
service packs, software updates via, 212
service principal name (SPN) suffix, 153
service requests, Active Directory sites, 108
Service (SRV) records, DNS, 129
services, managing, 28
share, creating software deployment, 219
shared folders, publishing, 88–89
shortcut trusts, 150
SID (security identifier), 47, 150
Simple Mail Transfer Protocol (SMTP),
 intersite replication, 118–120
single-master operations, 145–148
single sign-on (SSO), Web Application
Proxy, 307
site-aware certificate enrollment, AD
Certificate Services, 244
site link bridges, intrasite replication,
120–122
site links, replication, 112–113, 120–122
sites. See Active Directory sites
Sites level, GPO processing, 186
SMTP (Simple Mail Transfer Protocol),
 intersite replication, 118–120
SNI (server name indication), Web proxy
service, 279
software deployment, through GPO
configuring settings, 224–229
deploying applications, 217–218
Group Policy Slow Link Detection, 220
overview of, 211
preparing for, 218–219
publishing/assigning applications,
220–222
software management life cycle, 211–213
software restriction policies, 219–220
software updates, 222–223
using AppLocker, 220
verifying installation, 223–224
what to check before you install, 212
Windows Installer, 213–217
Software Installation Properties dialog box,
225–228
software management life cycle, 211–213
software restriction policies, 219–220
Software Restriction Policy, 185
Software Settings, Group Policy, 182
Software Update Services (SUS), 212
SPN (service principal name) suffix, 153
SRV (Service) records, DNS, 129
SSL certificates, 258, 295
SSO (single sign-on), Web Application
Proxy, 307
staging folder, DFSR, 111
stand-alone CAs, 249
Starter GPOs, Group Policy, 184
static IP addresses, Windows Azure VMs not
supporting, 24
strategies, group, 75
structure, OU
 creating, 53–57
 mapping to business needs, 50
 modifying, 57–58
 troubleshooting, 63
subdomains, 136–137, 140–141
subnets
 as Active Directory replication objects,
112–113
 creating, 115–116
 planning your sites, 110
 sites as collections of well-connected, 108
subordinate CAs, 248–250
SUS (Software Update Services), 212
switches
 Auditpol.exe, 189
gpresult, 234–235
GPPolicyImport, 193–194
synchronization, troubleshooting replication,
 130–131
system log, Event Viewer information
on, 26
System Monitor, 130
System State data, backup/restore,
160–162
Sysvol directory, backup, 160
TCP/IP, 29, 115–116
templates
AD Rights Management Services, 299–301, 305–306
certificate, 204, 260–264
creating user, 67–69
Group Policy administrative, 181
transform claims rule, 286
testing
Active Directory by clients, 29–30
basic network connectivity, 7–8
network configuration, 8–10
TGS-REP (ticket-granting service reply), AD Federation Services, 290
TGS-REQ (ticket-granting service request), AD Federation Services, 290
TGS (ticket-granting service) request, AD Federation Services, 290
TGT (ticket-granting ticket), AD Federation Services, 290
third-party products
Active Directory backups, 158
creating application data partitions, 31
Windows Installer specifications for, 213
TLS/SSL (Schannel SSP), 46
token decrypting certificate, AD FS, 285–286
token signing certificate, AD FS, 285–286
topology
configuring server, 125–127
troubleshooting replication, 131–132
TPD (trusted publishing domain), 302, 304–305
TraceRT command, network connectivity, 9
transform claims rule, AD Federation Services, 286, 288–289
transitive trusts, 137, 139, 149
trees. See domain trees and forests
troubleshooting
Active Directory replication, 129–132
OUs, 62–63
troubleshooting, Group Policies
gpresult.exe, 234–235
Infrastructure Dashboard, 236
overview of, 229–230
Resultant Set of Policy, 230–234
trust policies, AD Rights Management Services, 302–305
trusted publishing domain (TPD), 302, 304–305
trusts. See also Active Directory Domains and Trusts tool
managing, 27
managing relationships, 152
special types of, 150–151
transitive, 137, 139, 149
types of, 149–150
TUD (trusted user domain), 302–304
two-way (bidirectional) trusts, 149
two-way transitive trust relationship, 137

U
UGMC (Universal Group Membership Caching), 128, 155
unidirectional replication, RDOCs, 124–125
universal groups, 75
update sequence number (USN) journal, DFSR, 111
updates
automatic Group Policy, 224
forcing GPO, 191–193
issues before Windows Installer, 214
software, 212, 222–223
using Windows Updates, 212
upgrades
existing domains and forests, 156
software, 222–223
Windows AD FS 2016, 281–282
UPN (user principal name), 67, 153
URLs, AD Rights Management Services, 294
user accounts
creating with templates, 67–69
disabling vs. deleting, 47, 73
managing, 28
migrating, 70
as security principal, 46
User objects
defined, 65
Group Policy settings for, 182–183
properties, 71–72
Security Settings section of GPOs, 185
User principal name (UPN), 67, 153
usernames, automatic certificate renewal, 259
Users container, Active Directory organization, 64
USN (update sequence number) journal, DFSR, 111

V
validation, certificate, 251
validity periods, certificate, 250–251
verification
Active Directory installation, 2–10
software installation, 223–224

W
WANs (wide area networks)
overview of, 105
restoring System State data, 8
using multiple domains, 133
WAP (Web Application Proxy)
authentication capabilities, 308
exam essentials, 311–312
exam objectives, 273
overview of, 306
pass-through authentication, 307–308
PowerShell commands, 309–311
publishing applications, 306
review Q & A, 313–314, 320
summary, 311
wbadmin commands, 170–171
Web enrollment, 245
Web proxy service, AD FS, 279
WIF (Windows Identity Foundation), AD FS, 279
Windows authorization claims, AD FS, 287–288
Windows Azure, 24
Windows Deployment Services, 46
Windows Installer
application installation issues before, 214
benefits of, 214–216
configuring settings, 229
file types, 216–217
managing software management life cycle, 213
overview of, 213
Windows Integrated authentication, certificates, 259
Windows Live ID, AD RMS trust policies, 302
Windows PowerShell. See PowerShell
Windows Server 2016 Backup utility
overview of, 158
restoring Active Directory, 164–167
setting up backup, 163–164
Windows Settings, Group Policy, 182–183
Windows Time service, 146
Windows token-based agent, AD FS role service, 278
Windows Update, 212, 224
WMI (Windows Management Instrumentation) scripts, 194
WorkPlace Join, AD Federation Services, 292–293
WSH (Windows Script Host), 199
WSUS (Windows Server Update Service), 212, 224