

Index

Note: **Boldface** numbers indicate illustrations and code.

A

- ACCESS, 97
- access checking, RACF, 9–10, **10**
- access control, 83–84, 199
 - APF-authorized libraries and, 106
 - approval before granting access, 196
 - EXECUTE, 98
 - logging access in, 193, 195
 - RACF databases and, 120
 - RESTRICTED attribute and, 90
 - reviewing access rights in, 193–194
 - role-based security in, 188–189, **188**
 - SURROGAT class and, 161, 162
 - SYS1.UADS data set and, 145
 - system catalogs and, 116
 - System Management Facility (SMF) and, 111
 - temporary access granted in, 94, **94**
 - undercutting and, 92
 - z/OS UNIX and, 66–67, 66
- access lists, 9
 - SEARCH and, 59, **59**
 - WARNING mode and, 61
- access rights review, 193–194
- ACCOUNT, 144–145, **145**
- accountability, 165
- ACF2, 3, 8
- add-on products, 197–200
- ADDCREATOR, 98–99, 100
- address spaces, 7–8, **8**
- ADDS, 31, 34–35
- ALTDSD, 31
- ALTER, 31, 32
- AMASPZAP, 156
- APF-authorized libraries, 21–22, 103–107
 - access control for, 106
 - adding and removing, 107
 - finding, 104
 - LPA, MLPA, FLPA libraries and, 104
 - mitigating risk of, using DSMON, 105–107
 - PROTECTED attribute for, 105–106
 - risk to security from, 103–104
 - Selected Data Sets (in DSMON) report to find, 104–105, **105**
 - universal access (UACC) and, 106
 - validating, 107
 - vendor products and, 107
- application security, 7
 - FACILITY class and, 52
 - failure of, using WARNING mode in, 63
 - production vs. nonproduction, segregation of, 159–160, 196
 - special-use programs and, 155–156
 - z/OS operating system separation of programs and, 7–8, **8**
- approval before granting access, 196
- architecture for security. *See* security architecture
- asterisk (*), general access, 9
- AUDIT, 31
- auditing, 2, 29–37, 165, 166, 195
 - access checking by, 9–10, **10**, 9
 - ALTERing, using ALTDSD and RALTER, 31
 - AUDIT keyword and, 31
 - automatic, 35
 - classes and, 32–34
 - data sets and, 33, 36
 - FACILITY class, 52
 - failures of RACF commands, using CMDVIOL, 35
 - GLOBALAUDIT operand in, 32
 - level of, 30
 - LOGOPTIONS in, 33
 - optional nature of, 29
 - profiles, changes to, ADDSD and RDEFINE, 31, 34–35
 - PROTECTALL option and, 35
 - reasons for, 30
 - resources at class level, 32–34

resources at profile level, 31–32
 retaining logs from, importance of, 35–36
 SETROPTS in, 33
 special privileges and, 31, 34
 System Management Facility (SMF), 30, 35–36, 110
 turning off, 33
 user activity, using UAUDIT, 31
 violations and warnings in, 31
 z/OS and, 29, 30
 z/OS UNIX and, 29, 70–71
 AUDITOR privilege, 13, 14–15, 16, 20, 50, 69, 91, 96
 auditors
 AUDITOR privilege and, 13, 14–15, 16, 20, 69, 91, 96
 OPERAUDIT and, 14–15
 SAUDIT and, 14–15
 authentication, 9
 Authorized Caller Table report, 25–26, **26**
 Authorized Program Facility. *See* APF-authorized libraries
 automatic logging, 35
 automating processes, 77

B

backstop profile, BPX, 72–73, 92–93
 batch mode commands, 74–79
 automating a process with, 77
 capturing results of, 76–77
 entering groups of RACF commands in, 78, **78**
 ISPF and, 76–79
 JCL and, 75, 76
 repeating an action with, 77–78, 77
 required use of, 79
 batch processing, 159–162
 batch IDs in, 160, **160**
 production JCL and personal data sets in, 160–161
 restricting UPDATE access to production data in, 162

segregating production from nonproduction applications in, 159–160, 196
 SURROGAT class access and, 161, 162
 undefined profiles and, 88–89
 best practices, 187–196
 BPX prefix, FACILITY class, 65, 72–73, 92–93
 Bypass Label Processing (BLP) FACILITY class and, 51, 139
 tape, 137–139, **138**, **139**

C

CA Technologies, 3, 8
 capturing results of batch commands, 76–77
 catalogs, system, 115–116, **115–116**
 catch all profile, 72–73, 92–93
 CBT, 182
 CD/DVD drives, 2
 centralized security, 163, 166–167
 change management for product JCL, 194–195
 CICS, 14, 66–67, 86, 91, 103, 116, 162, 164, 191
 Class Descriptor Table (CDT), 16
 Class Descriptor Table report, 23–24, **24**
 classes
 access control to, 16
 CICS, 91
 Class Descriptor Table (CDT) and, 16
 DASDVOL, 17
 FACILITY, 49–53. *See also* FACILITY class, 49
 grouping, 91
 PROGRAM, 156
 resource auditing at, 32–34
 STARTED, 131–132
 SURROGAT, 161, 162
 z/OS UNIX and, auditing, 70–71
 CLISTs, 178
 cloning user IDs, 189
 CMDVIOL, 35

commands
 batch mode, 75–79
 native RACF, 183
 SEARCH command to create, 56, **56**
 compliance issues, 2–3, 185–186, 200
 Computer Associates International. *See* CA Technologies
 CONTROL, 32, 97
 corruption of RACF database, 119–120
 Covey, Stephen, 177
 critical data, 191

D

daemons, 72, 131
 DASDVOL class, 17
 data security, 3
 Data Security Monitor (DSMON), 19–28
 APF-authorized libraries and, 21–22, 104–107
 AUDITOR privilege and, 20
 finding users with special privileges using, 15–16, **15**
 Global Access Checking (GAC) table and, 42–43
 Global Access Table report in, using RACGAC, 22–23, 42–43
 Group Tree report in, using RACGRP, 27–28, **28**
 limitations of, 19
 operating system data sets reports in, using SYSSDS, 22
 Program Properties Table report in, using SYSPT, 25, 152–153, **152**
 RACF Authorized Caller Table report in, using RACAUT, 25–26, **26**
 RACF Class Descriptor Table report in, using RACCNT, 23–24, **24**
 RACF database report in, using RACDST, 22

- RACF Exits report in, using RACEXT, 25, 124–126, **125**
- RACF Started Procedures
Table reports in, using RACSPT, 23, 133–135, **133**
- reports generated from, 19–20
- Selected Data Sets report in, using SYSLNK, 21, 104–105, **105**, 115–116, **115–116**
- Selected User Attribute report in, using RACUSR, 21
- system catalogs and, 115–116, **115–116**
- system catalogs report in, using SYSCAT, 22
- system exits not reported by, 128
- System report in, using SYSTEM, 26–27, **27**
- uncluttering the security database with, 190
- understanding reports from, 20–23
- universal access (UACC) and, 21, 24
- using, 17
- data sets, 116–117
- auditing and, 33, 36
- fully-qualified generic profiles and, 94–95, 120–121, **120**, **121**
- operating system, 113–117
- partitioned, 141
- SYS1.UADS, 141–145
- System Management Facility (SMF) and, 111
- database cleanup, SEARCH command for, 56–57, **57**
- database de-cluttering, 190
- databases, RACF, 119–122
- access control for, 120
- corruption of, 119–120, 119
- fully-qualified generic profiles and, 120–121, **120**, **121**
- protecting, 120–121
- risks for, 119–120
- RVARY and, 120, 122, **122**
- unload type. *See* unload RACF databases
- DATASET class, 42, 89
- FACILITY class and, 49
- Global Access Checking (GAC) table and, 39–40, 45
- GLOBALAUDIT operand in, 32
- grouping unallowed in, 91
- masked entries in, 47
- z/OS UNIX and, 66
- DB2, 101, 103, 116, 162, 164, 191
- special privileges in, 14
- unload RACF databases and, uploading from, 171
- decentralized security, 166–167
- DEFAULT USER, z/OS UNIX and, 72
- DFHSM, 88
- DFSORT, 171, 183
- unload RACF databases and, 172–173, 176
- diagram showing access checking in RACF, **10**
- DIRACC, 70
- DIRSRCH, 70
- disaster recovery, 90–91
- discrete profiles, 87–88, **88**
- SEARCHing for, 59, **59**
- display, System Display and Search Facility (SDSF), 147–149
- Distributed Computing Environment (DCE), FACILITY class and, 51
- documentation of FACILITY class, 52
- DSMON. *See* Data Security Monitor
- E**
- edit capabilities of ISPF, 178–180, **179**
- employee transfers and terminations, 190–191
- enforcement of security compliance, 200. *See also* compliance issues
- Enron, 2, 185
- erasing disks, 155
- event logging, 29–37. *See also* auditing
- EXCLUDE, 178–180, **179**
- executable assembler load modules, 156
- EXECUTE, 98
- Exits report, 25, 124–126, **125**
- exits, RACF, 9, 123–126
- exits, system, 127–129, 127
- external security and RACF, 163, 164–165, 193
- F**
- FACILITY class, 49–53
- auditing, 52
- BPX prefix and, 65, 72–73, 92–93
- Bypass Label Processing (BLP) and, 51, 139
- cautions for, 53
- DATASET class and, 49
- Distributed Computing Environment (DCE) and, 51
- documentation in, 52
- ICHBLP profile and, 51, 139
- in-house developed products and, 52
- RACF and, 49
- RACF profiles and, 51
- security administration of profiles in, 52
- services protected by, 50
- STGADMIN and, 50, 51
- storage management and, 49–51
- third-party vendor products and, 52
- UNIX profiles and, 50, 51
- z/OS operating system and, 49, 50, 51
- z/OS UNIX and, 65, 69, 71–73
- failures of RACF commands, auditing, using CMDVIOL, 35

File Security Packets (FSPs), 66–67
FIND, 178–180, **179**
FIRECALL user ID, 161
flat files, 121, 169
FLPA libraries, 104
formatting tapes, 155
FSOBJ, 70
FSSEC, 70
FTP, z/OS UNIX and, 68
fully-qualified generic profiles, 94–95
 SYS1.UADS data set and, 145

G

general access, 9
generation data group (GDG)
 organization of records, in SMF, 112
GENERIC keyword, 88
generic profiles, 88
 fully-qualified, 94–95, 145
Global Access Checking (GAC)
 table, 9, 23, 39–47
 access levels for, 39
 access requests to, 39–41
 benefits of, 40
 candidates for processing by, 45–46
 Data Security Monitor (DSMON) reports and, 42–43
 DATASET class in, 39–40, 42, 45
 evaluating the security of, 47
 Global Access Table report for, 22–23, 42–43
 GLOBAL class and, 41–42
 implementing, 41–42
 masked dataset entries and, 47
 memory usage of, 40
 mirror profiles and, 43–44
 mitigating security risks of, 42–44
 profiles in, 39
 RESTRICTED attribute and, 39
 RLIST command in, 43
 SEARCH command in, 43

 security concerns of, 40–41
 setting up, 40
 System Management Facility (SMF) and, 41
Global Access Table report, 22–23, 42–43
GLOBAL class, 41–42
global options in RACF, 14, 96
GLOBALAUDIT operand, 32
granting access, 196
group IDs
 duplicates, finding with SEARCH, 58–59, **59**
 z/OS UNIX and, 66–67, 68–69, **68**

group-level special privileges, 13
Group Tree report, 27
grouping classes, 91
groups, 11, 53, 188–189, **188**, 194
 listing with SEARCH, 57, **57**
 OMVS segment of user ID in, 66–67, 69, 74
GROUP–SPECIAL, 51

H

HELP command, 60
Help Desk, 51
help functions in RACF, 181
Hierarchical File System (HFS), z/OS UNIX, 66, 74
HSM, 17

I

IBM Systems Magazine, 182
IBMUSER, 97–98
ICETOOL, 171
ICHBLP profile, 51, 139
ICHRIN03 table, started procedures and, 131–133
ICKDSF, 155
identifying important data, 191–192
IEHINITT, 155
IMASPZAP, 156
implementing security, 2
IMS, 14, 101, 103, 116, 162
in-house developed products, FACILITY class and, 52

infrastructure for security, 4, 157
initial program load (IPL), 113–114
initializing tapes, 155
inquisitive mindset, in security administration, 84–86
internal security in, 164–165, 193
IPCOBJ, 70
IRR.LISTUSER profile, 51
ISPF, 2, 171, 178, 183, 198
 batch mode commands and, 76–79
 edit capabilities of, 178–180, **179**

J

JCL, 2, 4, 170–171, **171**, 183
 batch mode commands and, 75, 76, 77
 change management for, 194–195
 production vs. personal data sets in, 160–161
JES, 113
JES exits, 127
JES2 started procedure, 132

L

label processing, BLP, 137–139, **138**, **139**
level of security, 81–82
LISTDSD, 96–97
logging activities, 29, 193–195.
 See also auditing
 OPERAUDIT for, 14–15
 SAUDIT for, 14–15
logon attempts, logging, 195
LOGOPTIONS, 33
LPA libraries, 104

M

mainframe security issues, 1–3, 7–12
masked dataset entries, GAC table and, 47
mentors, 180–181
Microsoft Access, 171
mirror profiles, GAC table and, 43–44

- MLPA libraries, 104
 monitoring security activities,
 195, 199
 MVS, 3
- N**
 NOADDCREATOR, 99
- O**
 OMEGAMON, 52
 OMVS segment of user ID,
 66–67, 69, 74
 online manuals, 181–182
 online user groups, 180
 OpenEdition MVS. *See* z/OS
 UNIX
 operating system data sets
 reports, 22
 operating system. *See* z/OS
 operating system
 operating systems, 3
 OPERATIONS privilege, 9, 11,
 13, 16–17, 34, 69, 91
 alternatives to, 16–17
 OPERAUDIT, 14–15
 OS/390, 3
 ownership of data, 192
- P**
 PARMLIB, 113
 partitioned data sets (PDS), 141
 passwords, 85–86, 200
 change interval for, 85–86, 96
 PASSWORD RESET and, 51
 RVARY and, RACF databases
 and, 122, **122**
 strength of, 95–96
 SYS1.UADS data set and, 142,
 144
 Payment Card Industry Data
 Security Standard (PCI
 DSS), 186
 PERMIT, 97, 139
 personal computer security
 issues, 1–3
 physical security, 2
 Physical Sequential (PS) format,
 in unload RACF databases,
 171
 PRIVILEGED attribute, 35
 started procedures and,
 131–135
 PROCACT, 70
 procedures, started. *See* started
 procedures
 PROCESS, 70
 PROCLIB, 113
 production data, 191
 productivity enhancement,
 177–183
 profiles, 194
 access levels in, 98
 asterisk for general access in, 9
 auditing and changes to,
 ADDSD and RDEFINE,
 34–35
 AUDITOR privilege and, 14
 backstop or catchall, BPX,
 72–73, 92–93
 BPX prefix and, 65
 creating, using ADDSD, 31,
 34–35
 creating, using RDEFINE, 31,
 34–35
 discrete, 59, **59**, 87–88, **88**
 FACILITY class and, 51, 53
 fully-qualified generic, 94–95,
 120–121, **120**, **121**, 145
 general access in, 9
 generic, 88
 Global Access Checking
 (GAC) table in, 9, 23,
 39–47. *See also* Global
 Access Checking (GAC)
 table
 GLOBALAUDIT operand
 in, 32
 ICHBLP profile and, 51, 139
 LISTDSD and, 96–97
 listing with SEARCH, 57, **57**
 mirrored, Global Access
 Checking (GAC) table and,
 43–44
 OPERATIONS privilege in,
 9, 11
 RACF, FACILITY class and,
 51
 resource auditing in, 31–32
 SEARCHing access to, 59, **59**
 segments in, 86–87, **86**
 storage administration,
 FACILITY class and, 50,
 51
 System Management Facility
 (SMF) and, 111
 universal access (UACC) in, 9,
 11, 89–90, 114
 unload RACF databases and,
 169
 WARNING mode for, 61, 63
 PROGRAM class, 156
 z/OS UNIX and, 74
 Program Properties Table (PPT),
 151–153
 Program Properties Table report,
 25, 152–153, **152**
 PROTECTALL option, 35
 PROTECTED, 105–106
- R**
 RACAUT, 25–26, **26**
 RACCDT, 23–24, **24**
 RACDST, 22
 RACEXT, 25
 RACF, 2, 3–4, 8, 9–12
 access lists in, 9
 backstop/catchall profiles in,
 92–93
 batch mode commands in,
 74–79
 classes within, access control
 and, 16
 commands in, 183
 DASDVOL class in, 17
 Data Security Monitor
 (DSMON) in. *See* Data
 Security Monitor
 databases in, 119–122. *See*
 databases, RACF
 diagram showing access
 checking in, **10**
 disaster recovery in, 90–91
 exits in, 9, 123–126. *See also*
 exits, RACF
 external security and, 163
 FACILITY class and, 49
 general access in, 9

- Global Access Checking (GAC) table in, 9, 23, 39–47. *See also* Global Access Checking (GAC) table
 - global option setting in, 14, 96
 - grouping classes in, 91
 - help functions in, 181
 - OPERATIONS privilege in, 9, 11
 - special privileges in. *See* Special privileges in RACF
 - SYS1.UADS data set and, 142–144
 - undercutting in, 92
 - universal access (UACC) in, 9, 11, 89–90, 114
 - z/OS UNIX and, 65–74. *See z/OS UNIX*
 - RACF Authorized Caller Table report, 25–26, **26**
 - RACF Class Descriptor Table report, 23–24, **24**
 - RACF database report, 22
 - RACF Exits report, 25, 124–126, **125**
 - RACF exits. *See* exits, RACF
 - RACF Started Procedures Table reports, 23, 133–135, **133**
 - RACF-L user group, 180
 - RACGAC, 22–23, 42–43
 - RACGRP, 27–28, **28**
 - RACSPT, 23
 - RACUSR, 21
 - RALTER, 31
 - RDEFINE, 31, 34–35
 - READ, 9, 11, 32
 - record types, unload RACF databases and, 169
 - repeating an action, batch mode commands, 77–78
 - reporting security activities, 195, 200
 - RESOURCE, 89
 - Resource Access Control Facility (RACF). *See* RACF
 - resource auditing
 - class level, 32–34
 - profile level, 31–32
 - RESTRICTED attribute, 39, 90
 - RESUME, 94
 - reviewing access rights, 193–194
 - REVOKE, 94
 - REVOKED, 91
 - revoking user IDs, 58, **58**, 84–85
 - REXX, 171, 176, 178
 - RJE, 89
 - RLIST, 43, 53
 - role-based security, 188–189
 - RVARY, 120, 122, **122**
 - S**
 - Sarbanes-Oxley (SOX) Act, 3, 185–186
 - SAS, 171, 176
 - SAUDIT, 14–15
 - SEARCH, 55–59
 - access to profiles and, 59, **59**
 - database cleanup using, 56–57, **57**
 - discrete profiles and, 59, **59**
 - finding duplicate UIDs/GIDs with, 58–59, **59**
 - Global Access Checking (GAC) table and, 43
 - listing profiles, user IDs, and groups with, 57, **57**
 - RACF command creation using, 56, **56**
 - reports using, 55
 - revoking user IDs with, 58, **58**
 - WARNING mode profiles using, 63
- search, in System Display and Search Facility (SDSF), 147–149
- security administration, 52, 81–100, 199
 - access control and, 83–84
 - inquisitive mindset required by, 84–86
 - lapses in, 83
 - level of security and, 81–82
 - “quick fixes” in, 83
 - role of, 82–84
 - skills required for, 82–84
 - user profile segments in RACF and, 86–87
 - security architecture, 163–167, 193
 - centralized security and, 163, 166–167
 - CICS and, 164
 - DB2 and, 164
 - decentralized security and, 166–167
 - external security and RACF in, 163, 164–165, 193
 - internal security in, 164–165, 193
 - System Display and Search Facility (SDSF) and, 164
 - third-party vendor products and, 164–165
 - segments in profiles, 86–87, **86**
 - segregating production from nonproduction applications in, 159–160, 196
 - Selected Data Sets report, 21, 104–105, **105**, 115–116, **115–116**
 - Selected User Attribute report, 21
 - SETOPTS, 37, 96, 98–99
 - auditing and, 33
 - global option setting using, 14
 - logging activities using, 14
 - SHARE, 183
 - shared user IDs, 93–94
 - SMF exits, 127
 - SORT JCL, unload RACF databases and, 172, **172**
 - SPECIAL privilege, 13, 14, 16, 34, 51, 69, 91, 96
 - special privileges, 13–17, 186, 199
 - alternatives to OPERATIONS in, 16–17
 - assigning, 15–16
 - auditing and, 31, 34
 - AUDITOR, 13, 14–15, 16, 20, 51, 69, 91, 96
 - DASDVOL class and, 17
 - disaster recovery and, 91
 - finding users with, using DSMON, 15–16, **15**
 - global option setting through, 14

- group level, 13
logging activities in, 14–15, 195
mitigating risk of, 15–16
OPERATIONS, 9, 11, 13, 16–17, 34, 69, 91
optional system components (DB2, CICS, IMS) and, 14
revoking, 15
SPECIAL, 13, 14, 16, 34, 51, 69, 91, 96
STGADMIN in, 17, 50, 51
SUPERUSER, 13, 69–70, **70**, 72, 74
system-wide, 13
TRUSTED procedures and, 17
UNIX. *See* z/OS UNIX
WARNING mode and, 61
special-use programs, 155–156
STARTED class, 131–132
z/OS UNIX and, 74
started procedures, 131–135
defining, with ICHRIN03 table, 131–132, **133**
DSMON report for, 23
mitigating risk of, 133–135, **133**
PRIVILEGED attribute in, 131, 132, 133–135
risks of, 132
STARTED class in, 131–132
Started Procedures Table reports in, 133–135, **133**
TRUSTED attribute in, 131, 132, 133–135
Started Procedures Table reports, 23, 133–135, **133**
started tasks. *See* started procedures
STGADMIN privilege, 17
FACILITY class and, 50, 51
HSM and, 17
STGADMIN privilege and, 17
storage management, FACILITY class and, 49
SUPERUSER privilege, 13, 69–70, **70**, 72, 74
SUPERZAP, 156
SURROGAT class access and, 161, 162
SYS1.UADS data set, 141–145
access control for, 145
brief history of, 142–143
fully-qualified generic profiles and, 145
keeping current with, TSO's ACCOUNT command in, 144–145, **145**
passwords and, 142, 144
RACF and, 142–144
TSO and, 142–145
universal access (UACC) and, 145
SYSCAT, 22
SYSLNK, 21
SYSPT, 25, 152–153, **152**
SYSSDS, 22
SYSTEM, 26–27, **27**
system catalogs, 22, 115–116, **115–116**
System Display and Search Facility (SDSF), 147–149, 164
system exits, 127–129. *See also* exits, RACF
System Management Facility (SMF), 109–112
access control for, 111
auditing and, 30, 35–36, 110
collecting records from, 110–111
data sets of, 111
generation data group (GDG) organization of records in, 112
Global Access Checking (GAC) table and, 41
mitigating risks of, 110–112
performance monitoring and, 110
profiles and, securing, 111
records found in, 109–110
retaining records from, 111
risks associated with, 110
security and, 109
system parameter libraries, 113–114
System report, 26–27, **27**
system-wide special privileges, 13
- T**
tape bypass label processing (BLP), 137–139, **138**, **139**
temporary access, 94, **94**
third-party vendor products, 164–165
APF-authorized libraries and, 107
FACILITY class and, 52
Top Secret, 3, 8
TRUSTED attribute, 35, 131–135
TRUSTED procedures, 17
TSO, 2, 4, 60, 66–67, 86, 141, 142, 143–145. *See also* SYS1.UADS data set
ACCOUNT command in, 144–145, **145**
ISPF. *See* ISPF
System Display and Search Facility (SDSF) and, 147–149
unload RACF databases and, 171, 173–175, **174**, **175**, 176
- U**
UACC. *See* universal access
UAUDIT, 31
undefined profiles, 88–89, **88**, **89**
undercutting, 92
universal access (UACC), 9, 11, 21, 24, 53, 89–90, 114, 183
APF-authorized libraries and, 106
SYS1.UADS data set and, 145
WARNING mode and, 61
z/OS UNIX and, 72
UNIX. *See* z/OS UNIX, 65
UNIXMAP class, 66, 68, 73
UNIXPRIV class, 66, 69–70, 71, 73
unload RACF databases, 121, 169–176

- before unload database, using LISTUSER, 170
 - benefits of, 171
 - creating, using a JCL, 170–171, **171**
 - DB2 and, uploading to, 171
 - DFSORT JCL for, 172–173, 176
 - exporting files from, 171
 - flat files in, 121, 169
 - languages supported by, 171
 - Physical Sequential (PS) format of, 171
 - profiles and, 169
 - protecting, 121
 - record types in, 169
 - reports from, 172–173
 - SORT JCL for, 172, **172**
 - TSO and, 171, 173–175, **174**, **175**, 176
 - UPDATE, 11, 32, 162
 - user activity auditing, using UAUDIT, 31
 - User Attribute Data Set. *See* SYS1.UADS data set
 - user groups, 180
 - user IDs, 9, 97–98, 188–189, 194
 - cloning, 189
 - duplicates, finding with SEARCH, 58–59, **59**
 - FIRECALL, 161
 - IBMUSER, 97–98
 - listing with SEARCH, 57, **57**
 - OMVS segment of, 66–67, 69, 74
 - RESTRICTED attribute on, 90
 - revoking, using SEARCH, 58, **58**, 84–85
 - sharing, 93–94
 - temporary access in, 94, **94**
 - undefined, 88–89, **88**, **89**
 - undercutting access in, 92
 - z/OS UNIX and, 66–67, 68–69, **68**
 - utility programs, 155–156, 182
- V**
- validation, 9
 - Vanguard Integrity Professionals, 198
 - Vanguard Security Conference, 183
 - vendor publications, 182
 - vendors. *See* third-party vendor products
 - violations/warnings, 195
 - auditing and, 31
 - Virtual Private Networks (VPN), 2
 - VSAM data sets, 97
 - VTAM, 113, 116
- W**
- WARNING mode, 61–64
 - cautions when using, 61–62
 - finding profiles that use, 63
 - “fixing” application failures with, 63
 - incorrect use of, 63
 - justifying use of, 64
 - removing, 64
 - temporary use of, 62
- Z**
- z/OS operating system, 3–4, 101, 191
 - address spaces in, 7–8, **8**
 - auditing in, 29, 30
 - authentication and validation in, 9
 - core security in, 8
 - data sets in, 113–117
 - exits in, 127–129. *See also* exits, RACF
 - FACILITY class and, 49, 50, 51
 - fully-qualified generic profiles and, 94–95, 120–121, **120**, **121**
 - initial program load (IPL) and, 113–114
 - logging in, 29
 - security products available for, 8. *See also* ACF2, Top Secret
 - separation of programs/applications within, 7–8, **8**
 - special-use programs and, 155–156
 - SYS1.UADS data set in, 141–145
 - system catalogs in, 115–116, **115–116**
 - system parameter libraries, 113–114
 - UNIX and. *See* z/OS UNIX
 - z/OS UNIX, 13, 86, 180
 - access and, 66–67
 - auditing, 29, 70–71
 - BPX prefix and, 65, 72–73, 92–93
 - daemons in, 72, 131
 - DATASET class and, 66
 - DEFAULT USER in, 72
 - FACILITY class and, 65, 69, 71–73
 - File Security Packets (FSPs) in, 66–67
 - FTP and, 68
 - group IDs and, 66–67, 68–69, **68**
 - Hierarchical File System (HFS) and, 66, 74
 - implementing controls in, 71
 - logging in, 29
 - OMVS segment of user ID in, 66–67, 69, 74, 86
 - planning for security using, 67–68
 - profiles in, FACILITY class and, 50, 51
 - PROGRAM class and, 74
 - security in, how it works, 66–67
 - STARTED class and, 74
 - SUPERUSER privilege and, 13, 69–70, **70**, 72, 74
 - universal access (UACC) and, 72
 - UNIXMAP class and, 66, 68, 70, 73
 - UNIXPRIV class and, 66, 69–70, **70**, 71, 73
 - user IDs and, 66–67, 68–69, **68**