EMC® Connectrix B Series Fabric OS Diagnostic and System Error Messages

Version 6.2

Reference Manual

P/N 300-008-686
REV A01

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.EMC.com

Published April, 2009

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.

Contents

Chapter 1 Introduction to System Messages

Overview of system messages 54
- System error message logging 54
- Event auditing 55
- System logging daemon (syslogd) 57
- System console 58
- Port logs 58

Viewing and configuring system message logs 59
- Viewing system messages from Web Tools 61
- Dumping system messages 61
- Viewing system messages one message at a time 62
- Clearing the system message log 63
- Configuring event auditing 64

Reading a RAS system message 65
- Audit event messages 66
- Message severity levels 68

Responding to a system message 69
- Looking up a system message 69
- Gathering information about the problem 69
- Support 70
- Panic dump and core dump files 70
- Trace dumps 71
- supportSave command 71

System module descriptions 72

PART 1 RASLog Messages

Chapter 2 AG System Messages

AG-1001 83
AG-1002 83
AG-1003 84
AG-1004 84
AG-1005 84
AG-1006 85
AG-1007 85
AG-1008 85
AG-1009 86
AG-1010 86
AG-1011 86
AG-1012 87
AG-1013 87
AG-1014 88
AG-1015 88
AG-1016 88
AG-1017 89
AG-1018 89
AG-1019 89
AG-1020 90
AG-1021 90
AG-1022 90
AG-1023 91
AG-1024 91
AG-1025 92
AG-1026 92
AG-1027 93
AG-1028 93
AG-1029 93

Chapter 3 AUTH System Messages

AUTH-1001 97
AUTH-1002 97
AUTH-1003 97
AUTH-1004 98
AUTH-1005 98
AUTH-1006 99
AUTH-1007 99
AUTH-1008 99
AUTH-1010 100
AUTH-1011 100

AUTH-1012 100
AUTH-1013 101
AUTH-1014 101
AUTH-1016 102
AUTH-1017 102
AUTH-1018 102
AUTH-1020 103
AUTH-1022 103
AUTH-1023 104
AUTH-1025 105
AUTH-1026 105
AUTH-1027 106
AUTH-1028 106
AUTH-1029 107
AUTH-1030 107
AUTH-1031 108
AUTH-1032 108
AUTH-1033 109
AUTH-1034 109
AUTH-1035 109
AUTH-1036 110
AUTH-1037 110
AUTH-1038 111
AUTH-1039 111
AUTH-1040 112
AUTH-1041 112
AUTH-1042 113
AUTH-1043 113
AUTH-1044 113

Chapter 4 BKSW System Messages

BKSW-1003 116

Chapter 5 BL System Messages

BL-1000 119
BL-1001 119
BL-1002 119
BL-1003 120
BL-1004 120
BL-1006 121
BL-1007 121

BL-1008 122
BL-1009 122
BL-1010 123
BL-1011 123
BL-1012 124
BL-1013 124
BL-1014 125
BL-1015 126
BL-1016 126
BL-1017 127
BL-1018 127
BL-1019 127
BL-1020 128
BL-1021 128
BL-1022 129
BL-1023 129
BL-1024 130
BL-1025 130
BL-1026 130
BL-1027 131
BL-1028 131
BL-1029 131
BL-1030 132
BL-1031 132
BL-1032 133
BL-1033 133
BL-1034 134
BL-1035 134
BL-1036 134
BL-1037 135

Chapter 6 BLL System Messages

BLL-1000 138

Chapter 7 BM System Messages

BM-1001 142
BM-1002 142
BM-1003 143
BM-1004 143
BM-1005 143
BM-1006 144

BM-1007 144
BM-1008 145
BM-1009 145
BM-1010 145
BM-1053 146
BM-1054 146
BM-1055 146
BM-1056 147
BM-1058 147

Chapter 8 C2 System Messages

C2-1001 150
C2-1002 150
C2-1004 150
C2-1005 151

Chapter 9 CDR System Messages

CDR-1001 154
CDR-1002 154
CDR-1003 154
CDR-1004 155

Chapter 10 CER System Messages

CER-1001 158

Chapter 11 CHASSIS System Messages

CHASSIS-1002 160
CHASSIS-1003 160
CHASSIS-1004 160
CHASSIS-1005 161

Chapter 12 CONF System Messages

CONF-1000 164
CONF-1001 164
CONF-1020 164
CONF-1021 165
CONF-1022 165
CONF-1030 165

Chapter 13 CTAP System Messages

CTAP-1001 168

Chapter 14 CVLC System Messages

CVLC-1001 170
CVLC-1002 170
CVLC-1003 170
CVLC-1004 171
CVLC-1005 171
CVLC-1006 171
CVLC-1008 172
CVLC-1009 172
CVLC-1010 172
CVLC-1011 173
CVLC-1012 173
CVLC-1013 174
CVLC-1014 174
CVLC-1015 174
CVLC-1016 175
CVLC-1017 175
CVLC-1018 175
CVLC-1019 176
CVLC-1020 176
CVLC-1021 176
CVLC-1022 177

Chapter 15 CVLM System Messages

CVLM-1001 180
CVLM-1002 180
CVLM-1003 180
CVLM-1004 181
CVLM-1005 181
CVLM-1006 181
CVLM-1007 182
CVLM-1008 182
CVLM-1009 182
CVLM-1010 183
CVLM-1011 183
CVLM-1012 183

Chapter 16 EM System Messages

EM-1001 187
EM-1002 187
EM-1003 187
EM-1004 188
EM-1005 188
EM-1006 189
EM-1007 189
EM-1008 190
EM-1009 190
EM-1010 191
EM-1011 191
EM-1012 191
EM-1013 192
EM-1014 192
EM-1015 193
EM-1016 193
EM-1017 193
EM-1018 194
EM-1019 194
EM-1028 194
EM-1029 195
EM-1031 195
EM-1033 196
EM-1034 196
EM-1035 197
EM-1036 197
EM-1037 198
EM-1041 198
EM-1042 199
EM-1043 199
EM-1044 199
EM-1045 200
EM-1046 200
EM-1047 201
EM-1048 201
EM-1049 202
EM-1050 202
EM-1051 202
EM-1055 203
EM-1056 203
EM-1057 203
EM-1058 204

EM-1059 204
EM-1060 205
EM-1061 205
EM-1062 205
EM-1063 206
EM-1064 206
EM-1065 207
EM-1066 207
EM-1067 207
EM-1068 208
EM-1069 208
EM-1070 209
EM-2003 209

Chapter 17 ESS System Messages

ESS-1001 212
ESS-1002 212
ESS-1003 213
ESS-1004 213
ESS-1005 214

Chapter 18 EVMD System Messages

EVMD-1001 216

Chapter 19 FABR System Messages

FABR-1001 219
FABR-1002 219
FABR-1003 219
FABR-1004 220
FABR-1005 220
FABR-1006 221
FABR-1007 221
FABR-1008 222
FABR-1009 222
FABR-1010 223
FABR-1011 223
FABR-1012 223
FABR-1013 224
FABR-1014 224
FABR-1015 225
FABR-1016 225

FABR-1017 226
FABR-1018 226
FABR-1019 226
FABR-1020 227
FABR-1021 227
FABR-1022 228
FABR-1023 228
FABR-1024 229
FABR-1029 229
FABR-1030 230
FABR-1031 230
FABR-1032 231
FABR-1034 231
FABR-1035 231
FABR-1036 232
FABR-1037 232
FABR-1038 233
FABR-1039 233
FABR-1040 233
FABR-1041 234
FABR-1043 234
FABR-1044 234
FABR-1045 235
FABR-1046 235

Chapter 20 FABS System Messages

FABS-1001 238
FABS-1002 238
FABS-1004 238
FABS-1005 239
FABS-1006 239
FABS-1007 240
FABS-1008 240
FABS-1009 241
FABS-1010 241
FABS-1011 241
FABS-1012 242
FABS-1013 242
FABS-1014 243
FABS-1015 243

Chapter 21 FBC System Messages

FBC-1001 246

Chapter 22 FCIP System Messages

FCIP-1000 248
FCIP-1001 248
FCIP-1002 248
FCIP-1003 249
FCIP-1004 249

Chapter 23 FCMC System Messages

FCMC-1001 252

Chapter 24 FCPD System Messages

FCPD-1001 254
FCPD-1002 254
FCPD-1003 255

Chapter 25 FCPH System Messages

FCPH-1001 258
FCPH-1002 258

Chapter 26 FCR System Messages

FCR-1001 262
FCR-1002 262
FCR-1003 262
FCR-1004 263
FCR-1005 263
FCR-1006 263
FCR-1007 264
FCR-1008 264
FCR-1009 264
FCR-1010 265
FCR-1011 265
FCR-1012 265
FCR-1013 266
FCR-1015 266
FCR-1016 266

FCR-1018 267
FCR-1019 267
FCR-1020 268
FCR-1021 268
FCR-1022 269
FCR-1023 269
FCR-1024 269
FCR-1025 270
FCR-1026 270
FCR-1027 271
FCR-1028 271
FCR-1029 272
FCR-1030 272
FCR-1031 273
FCR-1032 273
FCR-1033 273
FCR-1034 274
FCR-1035 274
FCR-1036 274
FCR-1037 275
FCR-1038 275
FCR-1039 275
FCR-1040 276
FCR-1041 276
FCR-1042 276
FCR-1043 277
FCR-1048 277
FCR-1049 277
FCR-1053 278
FCR-1054 278
FCR-1055 279
FCR-1056 279
FCR-1057 279
FCR-1058 280
FCR-1059 280
FCR-1060 281
FCR-1061 281
FCR-1062 282
FCR-1063 282
FCR-1064 282
FCR-1065 283
FCR-1066 283
FCR-1067 284

FCR-1068 284
FCR-1069 284
FCR-1070 285
FCR-1071 285
FCR-1072 285
FCR-1073 286
FCR-1074 286
FCR-1075 287
FCR-1076 287
FCR-1077 287
FCR-1078 288
FCR-1079 288
FCR-1080 289
FCR-1081 289
FCR-1082 289
FCR-1083 290
FCR-1084 290
FCR-1085 291
FCR-1086 291
FCR-1087 291
FCR-1088 292
FCR-1089 292

Chapter 27 FICN System Messages

FICN-1003 297
FICN-1004 297
FICN-1005 297
FICN-1006 298
FICN-1007 298
FICN-1008 298
FICN-1009 299
FICN-1010 299
FICN-1011 300
FICN-1012 300
FICN-1013 300
FICN-1014 301
FICN-1015 301
FICN-1016 301
FICN-1017 302
FICN-1018 302
FICN-1019 302
FICN-1020 303

FICN-1021 303
FICN-1022 304
FICN-1023 304
FICN-1024 304
FICN-1025 305
FICN-1026 305
FICN-1027 305
FICN-1028 306
FICN-1029 306
FICN-1030 307
FICN-1031 307
FICN-1032 307
FICN-1033 308
FICN-1034 308
FICN-1035 308
FICN-1036 309
FICN-1037 309
FICN-1038 309
FICN-1039 310
FICN-1040 310
FICN-1041 310
FICN-1042 311
FICN-1043 311
FICN-1044 312
FICN-1045 312
FICN-1046 312
FICN-1047 313
FICN-1048 313
FICN-1049 313
FICN-1050 314
FICN-1051 314
FICN-1052 314
FICN-1053 315
FICN-1054 315
FICN-1055 315
FICN-1056 316
FICN-1057 316
FICN-1058 316
FICN-1059 317
FICN-1060 317
FICN-1061 317
FICN-1062 318
FICN-1063 318

FICN-1064 319
FICN-1065 319
FICN-1066 319
FICN-1067 320
FICN-1068 320
FICN-1069 320
FICN-1070 321
FICN-1071 321
FICN-1072 321
FICN-1073 322
FICN-1074 322
FICN-1075 323
FICN-1076 323
FICN-1077 324
FICN-1078 324
FICN-1079 325
FICN-1080 325
FICN-1081 326
FICN-1082 326
FICN-1083 326
FICN-1084 327
FICN-1085 327
FICN-1086 327

Chapter 28 FICU System Messages

FICU-1001 330
FICU-1002 330
FICU-1003 330
FICU-1004 331
FICU-1005 332
FICU-1006 332
FICU-1007 332
FICU-1008 333
FICU-1009 333
FICU-1010 334

Chapter 29 FKLB System Messages

FKLB-1001 336

Chapter 30 FLOD System Messages

FLOD-1001 338

FLOD-1003 338
FLOD-1004 338
FLOD-1005 339
FLOD-1006 339

Chapter 31 FSPF System Messages

FSPF-1001 342
FSPF-1002 342
FSPF-1003 342
FSPF-1005 343
FSPF-1006 343

Chapter 32 FSS System Messages

FSS-1001 346
FSS-1002 346
FSS-1003 346
FSS-1004 347
FSS-1005 347
FSS-1006 348
FSS-1007 348
FSS-1008 348
FSS-1009 349
FSS-1010 349
FSS-1011 349

Chapter 33 FSSM System Messages

FSSM-1002 352
FSSM-1003 352
FSSM-1004 352

Chapter 34 FW System Messages

FW-1001 361
FW-1002 361
FW-1003 362
FW-1004 362
FW-1005 362
FW-1006 363
FW-1007 363
FW-1008 364
FW-1009 364

FW-1010 364
FW-1011 365
FW-1012 365
FW-1033 366
FW-1034 366
FW-1035 366
FW-1036 367
FW-1037 367
FW-1038 368
FW-1039 368
FW-1040 368
FW-1041 369
FW-1042 369
FW-1043 370
FW-1044 370
FW-1045 371
FW-1046 371
FW-1047 371
FW-1048 372
FW-1049 372
FW-1050 373
FW-1051 373
FW-1052 373
FW-1113 374
FW-1114 374
FW-1115 375
FW-1116 375
FW-1117 376
FW-1118 376
FW-1119 377
FW-1120 377
FW-1121 378
FW-1122 378
FW-1123 379
FW-1124 379
FW-1125 379
FW-1126 380
FW-1127 381
FW-1128 381
FW-1129 382
FW-1130 382
FW-1131 382
FW-1132 383

FW-1133 383
FW-1134 384
FW-1135 384
FW-1136 384
FW-1137 385
FW-1138 385
FW-1139 386
FW-1140 386
FW-1160 386
FW-1161 387
FW-1162 387
FW-1163 388
FW-1164 388
FW-1165 389
FW-1166 389
FW-1167 390
FW-1168 390
FW-1169 391
FW-1170 391
FW-1171 391
FW-1172 392
FW-1173 392
FW-1174 393
FW-1175 393
FW-1176 394
FW-1177 394
FW-1178 394
FW-1179 395
FW-1180 395
FW-1181 396
FW-1182 396
FW-1183 396
FW-1184 397
FW-1185 397
FW-1186 398
FW-1187 398
FW-1188 398
FW-1189 399
FW-1190 399
FW-1191 399
FW-1192 400
FW-1193 400
FW-1194 401

FW-1195 401
FW-1196 401
FW-1197 402
FW-1198 402
FW-1199 403
FW-1216 403
FW-1217 404
FW-1218 404
FW-1219 405
FW-1240 405
FW-1241 406
FW-1242 406
FW-1243 407
FW-1244 407
FW-1245 408
FW-1246 408
FW-1247 408
FW-1248 409
FW-1249 409
FW-1250 410
FW-1251 410
FW-1272 410
FW-1273 411
FW-1274 411
FW-1275 412
FW-1296 412
FW-1297 413
FW-1298 413
FW-1299 414
FW-1300 414
FW-1301 415
FW-1302 415
FW-1303 416
FW-1304 416
FW-1305 417
FW-1306 417
FW-1307 418
FW-1308 418
FW-1309 419
FW-1310 419
FW-1311 419
FW-1312 420
FW-1313 420

FW-1314 421
FW-1315 421
FW-1316 422
FW-1317 422
FW-1318 423
FW-1319 423
FW-1320 424
FW-1321 424
FW-1322 425
FW-1323 425
FW-1324 426
FW-1325 426
FW-1326 426
FW-1327 427
FW-1328 427
FW-1329 428
FW-1330 428
FW-1331 429
FW-1332 429
FW-1333 430
FW-1334 430
FW-1335 431
FW-1336 431
FW-1337 432
FW-1338 432
FW-1339 433
FW-1340 433
FW-1341 434
FW-1342 434
FW-1343 434
FW-1344 435
FW-1345 435
FW-1346 436
FW-1347 436
FW-1348 437
FW-1349 437
FW-1350 438
FW-1351 438
FW-1352 439
FW-1353 440
FW-1354 440
FW-1355 441
FW-1356 441

FW-1357 442
FW-1358 442
FW-1359 443
FW-1360 443
FW-1361 444
FW-1362 444
FW-1363 444
FW-1364 445
FW-1365 445
FW-1366 446
FW-1367 446
FW-1368 446
FW-1369 447
FW-1370 447
FW-1371 448
FW-1372 448
FW-1373 449
FW-1374 449
FW-1375 450
FW-1376 450
FW-1377 451
FW-1378 451
FW-1379 452
FW-1400 452
FW-1401 453
FW-1402 453
FW-1403 454
FW-1424 454
FW-1425 454
FW-1426 455
FW-1427 455
FW-1428 455
FW-1429 456
FW-1430 456
FW-1431 456
FW-1432 457
FW-1433 457
FW-1434 458
FW-1435 458
FW-1436 458
FW-1437 459
FW-1438 459
FW-1439 460

FW-1440 460
FW-1441 460
FW-1442 461
FW-1443 461
FW-1444 461
FW-1445 462
FW-1446 462
FW-1500 463
FW-1501 463
FW-1510 463

Chapter 35 HAM System Messages

HAM-1001 466
HAM-1002 466
HAM-1004 466
HAM-1005 467
HAM-1006 468
HAM-1007 468
HAM-1008 469
HAM-1009 469

Chapter 36 HAMK System Messages

HAMK-1001 472
HAMK-1002 472
HAMK-1003 472
HAMK-1004 473

Chapter 37 HIL System Messages

HIL-1101 477
HIL-1102 477
HIL-1103 477
HIL-1104 478
HIL-1105 478
HIL-1106 478
HIL-1107 479
HIL-1108 479
HIL-1201 480
HIL-1202 480
HIL-1203 481
HIL-1204 481

HIL-1206 482
HIL-1207 482
HIL-1208 483
HIL-1301 483
HIL-1302 483
HIL-1303 484
HIL-1304 484
HIL-1305 484
HIL-1306 485
HIL-1307 485
HIL-1308 485
HIL-1309 486
HIL-1310 486
HIL-1311 486
HIL-1401 487
HIL-1402 487
HIL-1403 487
HIL-1404 488
HIL-1501 488
HIL-1502 488
HIL-1503 489
HIL-1504 489
HIL-1505 490
HIL-1506 490
HIL-1507 491
HIL-1508 491
HIL-1509 492
HIL-1510 492
HIL-1601 493
HIL-1602 493
HIL-1603 493
HIL-1610 494
HIL-1650 494

Chapter 38 HLO System Messages

HLO-1001 496
HLO-1002 496
HLO-1003 497

Chapter 39 HMON System Messages

HMON-1001 500

Chapter 40 HTTP System Messages

HTTP-1001 502
HTTP-1002 502
HTTP-1003 502

Chapter 41 IBD System Messages

IBD-1001 504

Chapter 42 IBPD System Messages

IBPD-1001 506
IBPD-1002 506
IBPD-1003 506

Chapter 43 ICPD System Messages

ICPD-1001 508
ICPD-1002 508
ICPD-1003 508
ICPD-1004 509
ICPD-1005 509
ICPD-1006 509
ICPD-1007 510
ICPD-1008 510

Chapter 44 IPAD System Messages

IPAD-1000 512
IPAD-1001 512

Chapter 45 IPS System Messages

IPS-1001 514
IPS-1002 514
IPS-1003 514
IPS-1004 515
IPS-1005 515
IPS-1006 516

Chapter 46 ISCS System Messages

ISCS-1000 518

Chapter 47 ISNS System Messages

ISNS-1001 520
ISNS-1002 520
ISNS-1003 520
ISNS-1004 521
ISNS-1005 521
ISNS-1006 521
ISNS-1008 522
ISNS-1009 522
ISNS-1010 522
ISNS-1011 523
ISNS-1013 523
ISNS-1014 523

Chapter 48 KAC System Messages

KAC-1002 526
KAC-1004 526
KAC-1006 526
KAC-1007 527
KAC-1008 527

Chapter 49 KSWD System Messages

KSWD-1001 530
KSWD-1002 530
KSWD-1003 530

Chapter 50 KTRC System Messages

KTRC-1001 534
KTRC-1002 534
KTRC-1003 534
KTRC-1004 535
KTRC-1005 535

Chapter 51 LFM System Messages

LFM-1001 538
LFM-1002 538
LFM-1003 538
LFM-1004 539
LFM-1005 539

LFM-1006 539

Chapter 52 LOG System Messages

LOG-1000 542
LOG-1001 542
LOG-1002 543
LOG-1003 543

Chapter 53 LSDB System Messages

LSDB-1001 546
LSDB-1002 546
LSDB-1003 547
LSDB-1004 547

Chapter 54 MFIC System Messages

MFIC-1001 550
MFIC-1002 550
MFIC-1003 551

Chapter 55 MPTH System Messages

MPTH-1001 554
MPTH-1002 554
MPTH-1003 554

Chapter 56 MQ System Messages

MQ-1004 556

Chapter 57 MS System Messages

MS-1001 558
MS-1002 558
MS-1003 559
MS-1004 560
MS-1005 560
MS-1006 561
MS-1008 561
MS-1009 562
MS-1021 562
MS-1022 563

MS-1023 563
MS-1024 563

Chapter 58 NBFS System Messages

NBFS-1001 566
NBFS-1002 566
NBFS-1003 567

Chapter 59 NS System Messages

NS-1001 570
NS-1002 570
NS-1003 571
NS-1004 571
NS-1005 572
NS-1006 572

Chapter 60 PDM System Messages

PDM-1001 574
PDM-1002 574
PDM-1003 574
PDM-1004 575
PDM-1005 575
PDM-1006 575
PDM-1007 576
PDM-1008 576
PDM-1009 577
PDM-1010 577
PDM-1011 577
PDM-1012 578
PDM-1013 578
PDM-1014 578
PDM-1017 579
PDM-1019 579
PDM-1020 580
PDM-1021 580
PDM-1022 580
PDM-1023 581
PDM-1024 581

Chapter 61 PDTR System Messages

PDTR-1001 584
PDTR-1002 584

Chapter 62 PLAT System Messages

PLAT-1000 586
PLAT-1001 586
PLAT-1002 587
PLAT-1003 587

Chapter 63 PMGR System Messages

PMGR-1001 590
PMGR-1002 590
PMGR-1003 590
PMGR-1004 590
PMGR-1005 591
PMGR-1006 591
PMGR-1007 591
PMGR-1008 592
PMGR-1009 592
PMGR-1010 592

Chapter 64 PORT System Messages

PORT-1003 596
PORT-1004 596
PORT-1005 597

Chapter 65 PS System Messages

PS-1000 600
PS-1001 600
PS-1002 600
PS-1003 601
PS-1004 601
PS-1005 601
PS-1006 602

Chapter 66 PSWP System Messages

PSWP-1001 604

PSWP-1002 604
PSWP-1003 604

Chapter 67 RAS System Messages

RAS-1001 606
RAS-1002 606
RAS-1004 606
RAS-1005 607
RAS-1006 607
RAS-2001 607
RAS-2002 608
RAS-2003 608
RAS-3001 608
RAS-3002 609
RAS-3003 609
RAS-3004 609

Chapter 68 RCS System Messages

RCS-1001 612
RCS-1002 612
RCS-1003 612
RCS-1004 613
RCS-1005 613
RCS-1006 614
RCS-1007 614
RCS-1008 615

Chapter 69 RKD System Messages

RKD-1001 618
RKD-1002 618
RKD-1003 618

Chapter 70 RPCD System Messages

RPCD-1001 622
RPCD-1002 622
RPCD-1003 622
RPCD-1004 623
RPCD-1005 623
RPCD-1006 623
RPCD-1007 624

Chapter 71 RTWR System Messages

RTWR-1001 626
RTWR-1002 626
RTWR-1003 627

Chapter 72 SAS System Messages

SAS-1001 630

Chapter 73 SCN System Messages

SCN-1001 632

Chapter 74 SEC System Messages

SEC-1001 638
SEC-1002 638
SEC-1003 639
SEC-1005 639
SEC-1006 640
SEC-1007 640
SEC-1008 641
SEC-1009 641
SEC-1016 641
SEC-1022 642
SEC-1024 642
SEC-1025 642
SEC-1026 643
SEC-1028 643
SEC-1029 644
SEC-1030 644
SEC-1031 645
SEC-1032 645
SEC-1033 645
SEC-1034 646
SEC-1035 646
SEC-1036 646
SEC-1037 647
SEC-1038 647
SEC-1040 647
SEC-1041 648
SEC-1042 648
SEC-1043 648

SEC-1044 649
SEC-1045 649
SEC-1046 650
SEC-1049 650
SEC-1050 650
SEC-1051 651
SEC-1052 651
SEC-1053 652
SEC-1054 652
SEC-1055 653
SEC-1056 653
SEC-1057 653
SEC-1059 654
SEC-1062 654
SEC-1063 655
SEC-1064 655
SEC-1065 655
SEC-1069 656
SEC-1071 656
SEC-1072 656
SEC-1073 657
SEC-1074 657
SEC-1075 657
SEC-1076 658
SEC-1077 658
SEC-1078 658
SEC-1079 659
SEC-1080 659
SEC-1081 660
SEC-1082 660
SEC-1083 660
SEC-1084 661
SEC-1085 661
SEC-1086 661
SEC-1087 662
SEC-1088 662
SEC-1089 662
SEC-1090 663
SEC-1091 663
SEC-1092 663
SEC-1093 664
SEC-1094 664
SEC-1095 665

SEC-1096 665
SEC-1097 665
SEC-1098 666
SEC-1099 666
SEC-1100 666
SEC-1101 667
SEC-1102 667
SEC-1104 668
SEC-1105 668
SEC-1106 668
SEC-1107 669
SEC-1108 669
SEC-1110 670
SEC-1111 670
SEC-1112 670
SEC-1113 671
SEC-1114 671
SEC-1115 671
SEC-1116 672
SEC-1117 672
SEC-1118 672
SEC-1119 673
SEC-1121 673
SEC-1122 673
SEC-1123 674
SEC-1124 674
SEC-1126 674
SEC-1130 675
SEC-1135 675
SEC-1136 675
SEC-1137 676
SEC-1138 677
SEC-1139 677
SEC-1142 677
SEC-1145 678
SEC-1146 678
SEC-1153 679
SEC-1154 679
SEC-1155 679
SEC-1156 680
SEC-1157 680
SEC-1158 681
SEC-1159 681

SEC-1160 681
SEC-1163 682
SEC-1164 682
SEC-1165 682
SEC-1166 683
SEC-1167 683
SEC-1168 683
SEC-1170 684
SEC-1171 684
SEC-1172 685
SEC-1173 685
SEC-1174 685
SEC-1175 686
SEC-1176 686
SEC-1180 686
SEC-1181 687
SEC-1182 687
SEC-1183 687
SEC-1184 688
SEC-1185 688
SEC-1186 688
SEC-1187 689
SEC-1188 689
SEC-1189 690
SEC-1190 690
SEC-1191 691
SEC-1192 691
SEC-1193 692
SEC-1194 692
SEC-1195 692
SEC-1196 693
SEC-1197 693
SEC-1198 694
SEC-1199 694
SEC-1200 695
SEC-1201 695
SEC-1202 696
SEC-1203 696
SEC-1250 696
SEC-1251 697
SEC-1253 697
SEC-1300 698
SEC-1301 698

SEC-1302 698
SEC-1303 699
SEC-1304 699
SEC-1305 699
SEC-1306 700
SEC-1307 700
SEC-1308 701
SEC-1309 701
SEC-1310 701
SEC-1311 702
SEC-1312 702
SEC-1313 702
SEC-1314 703
SEC-1315 703
SEC-1316 704
SEC-1317 704
SEC-1318 704
SEC-1319 705
SEC-1320 705
SEC-1321 705
SEC-1322 706
SEC-1323 706
SEC-1324 706
SEC-1325 707
SEC-1326 707
SEC-1327 708
SEC-1328 708
SEC-1329 708
SEC-1330 709
SEC-1331 709
SEC-1332 710
SEC-1333 710
SEC-3035 710
SEC-3036 711
SEC-3037 711
SEC-3038 711
SEC-3039 712
SEC-3050 712
SEC-3051 712

Chapter 75 SNMP System Messages

SNMP-1001 716

SNMP-1002 716
SNMP-1003 716
SNMP-1004 717
SNMP-1005 717
SNMP-1006 717
SNMP-1007 718
SNMP-1008 718

Chapter 76 SPC System Messages

SPC-1001 721
SPC-1002 721
SPC-1003 721
SPC-2001 722
SPC-2002 722
SPC-2003 722
SPC-2004 723
SPC-2005 723
SPC-2006 723
SPC-2007 724
SPC-2008 724
SPC-2009 724
SPC-2010 725
SPC-2011 725
SPC-2012 725
SPC-3001 726
SPC-3002 726
SPC-3003 726
SPC-3004 727
SPC-3005 727
SPC-3006 728
SPC-3007 728
SPC-3008 729
SPC-3009 729
SPC-3010 730
SPC-3011 730
SPC-3012 730
SPC-3013 731
SPC-3014 731
SPC-3015 732

Chapter 77 SPM System Messages

SPM-1001 734
SPM-1002 734
SPM-1003 734
SPM-1004 734
SPM-1005 735
SPM-1006 735
SPM-1007 735
SPM-1008 736
SPM-1009 736
SPM-1010 736

Chapter 78 SS System Messages

SS-1000 740
SS-1001 740
SS-1002 741
SS-1003 741

Chapter 79 SULB System Messages

SULB-1001 745
SULB-1002 745
SULB-1003 745
SULB-1004 746
SULB-1005 746
SULB-1006 746
SULB-1007 747
SULB-1008 747
SULB-1009 747
SULB-1010 756
SULB-1011 756
SULB-1017 757
SULB-1018 757
SULB-1020 757
SULB-1021 758
SULB-1022 758
SULB-1023 759
SULB-1024 759
SULB-1025 760
SULB-1026 760
SULB-1030 760
SULB-1031 761

SULB-1032 761
SULB-1033 761
SULB-1034 762
SULB-1035 762
SULB-1036 762
SULB-1037 763

Chapter 80 SWCH System Messages

SWCH-1001 766
SWCH-1002 766
SWCH-1003 766
SWCH-1004 767
SWCH-1005 767
SWCH-1006 768
SWCH-1007 768
SWCH-1008 769
SWCH-1009 769
SWCH-1010 770
SWCH-1011 770

Chapter 81 SYSC System Messages

SYSC-1001 772
SYSC-1002 772
SYSC-1003 773
SYSC-1004 773
SYSC-1005 774

Chapter 82 SYSM System Messages

SYSM-1001 776
SYSM-1002 776
SYSM-1003 776
SYSM-1004 777
SYSM-1005 777
SYSM-1006 777
SYSM-1007 778

Chapter 83 TAPE Messages

TAPE-1001 780

Chapter 84 TRCE System Messages

TRCE-1001 782
TRCE-1002 782
TRCE-1003 783
TRCE-1004 783
TRCE-1005 783
TRCE-1006 784
TRCE-1007 784
TRCE-1008 784
TRCE-1009 785
TRCE-1010 785
TRCE-1011 786
TRCE-1012 786

Chapter 85 TRCK System Messages

TRCK-1001 788
TRCK-1002 788
TRCK-1003 788
TRCK-1004 789
TRCK-1005 789
TRCK-1006 789

Chapter 86 TS System Messages

TS-1001 792
TS-1002 792
TS-1006 793
TS-1007 793
TS-1008 794

Chapter 87 UCST System Messages

UCST-1003 796
UCST-1007 796
UCST-1020 796
UCST-1025 797
UCST-1026 797
UCST-1027 797

Chapter 88 UPTH System Messages

UPTH-1001 800

Chapter 89 WEBD System Messages

WEBD-1001 802
WEBD-1002 802
WEBD-1004 802
WEBD-1005 803
WEBD-1006 803
WEBD-1007 803
WEBD-1008 804

Chapter 90 ZOLB System Messages

ZOLB-1001 806

Chapter 91 ZONE System Messages

ZONE-1002 809
ZONE-1003 809
ZONE-1004 809
ZONE-1005 810
ZONE-1006 811
ZONE-1007 811
ZONE-1008 812
ZONE-1010 812
ZONE-1012 812
ZONE-1013 813
ZONE-1014 813
ZONE-1015 813
ZONE-1017 814
ZONE-1018 814
ZONE-1019 815
ZONE-1022 815
ZONE-1023 816
ZONE-1024 816
ZONE-1026 816
ZONE-1027 817
ZONE-1028 817
ZONE-1029 818
ZONE-1030 818
ZONE-1031 819
ZONE-1032 819
ZONE-1033 819
ZONE-1034 820
ZONE-1035 820

ZONE-1036 820
ZONE-1037 821
ZONE-1038 821
ZONE-1039 821
ZONE-1040 822
ZONE-1041 822
ZONE-1042 822
ZONE-1043 823
ZONE-1044 823
ZONE-1045 823
ZONE-1046 824
ZONE-1047 824
ZONE-1048 824
ZONE-1049 825
ZONE-1050 825
ZONE-1051 825
ZONE-1052 826
ZONE-1053 826

PART 2 Audit Log Messages

Chapter 92 AUDIT AG System Messages

AG-1029 830

Chapter 93 AUDIT AUTH System Messages

AUTH-3001 832
AUTH-3002 832
AUTH-3003 832
AUTH-3004 833
AUTH-3005 833
AUTH-3006 834
AUTH-3007 834
AUTH-3008 835

Chapter 94 AUDIT CONF System Messages

CONF-1000 838
CONF-1020 838
CONF-1022 838

Chapter 95 AUDIT FCIP System Messages

FCIP-1002 842
FCIP-1003 842

Chapter 96 AUDIT FICU System Messages

FICU-1011 844
FICU-1012 844

Chapter 97 AUDIT FW System Messages

FW-3001 846

Chapter 98 AUDIT HTTP System Messages

HTTP-1002 848
HTTP-1003 848

Chapter 99 AUDIT IPAD System Messages

IPAD-1002 850

Chapter 100 AUDIT PORT System Messages

PORT-1006 852
PORT-1007 852
PORT-1008 852
PORT-1009 853

Chapter 101 AUDIT SEC System Messages

SEC-3001 857
SEC-3002 857
SEC-3003 858
SEC-3004 858
SEC-3005 858
SEC-3006 859
SEC-3007 859
SEC-3008 860
SEC-3009 860
SEC-3010 861
SEC-3011 861
SEC-3012 861

SEC-3013 862
SEC-3014 862
SEC-3015 863
SEC-3016 863
SEC-3017 863
SEC-3018 864
SEC-3019 864
SEC-3020 865
SEC-3021 865
SEC-3022 865
SEC-3023 866
SEC-3024 866
SEC-3025 866
SEC-3026 867
SEC-3027 867
SEC-3028 867
SEC-3029 868
SEC-3030 868
SEC-3031 869
SEC-3032 869
SEC-3033 869
SEC-3034 870
SEC-3035 870
SEC-3036 870
SEC-3037 871
SEC-3038 871
SEC-3039 872
SEC-3040 872
SEC-3041 872
SEC-3044 873
SEC-3045 873
SEC-3046 873
SEC-3047 874
SEC-3048 874
SEC-3049 874
SEC-3050 875
SEC-3051 875

Chapter 102 AUDIT SNMP System Messages

SNMP-1004 878
SNMP-1005 878
SNMP-1006 878

Chapter 103 AUDIT SULB System Messages

SULB-1001 ... 882
SULB-1002 ... 882
SULB-1003 ... 882
SULB-1004 ... 883
SULB-1009 ... 883
SULB-1010 ... 891
SULB-1017 ... 892
SULB-1018 ... 892
SULB-1020 ... 893
SULB-1021 ... 893
SULB-1023 ... 894
SULB-1024 ... 894
SULB-1026 ... 895
SULB-1030 ... 895
SULB-1031 ... 896
SULB-1032 ... 896
SULB-1033 ... 896
SULB-1034 ... 897
SULB-1035 ... 897
SULB-1037 ... 898

Chapter 104 AUDIT SWCH System Messages

SWCH-1012 ... 900
SWCH-1013 ... 900
SWCH-1014 ... 900

Chapter 105 AUDIT UCST System Messages

UCST-1021 ... 904
UCST-1022 ... 904
UCST-1023 ... 904
UCST-1024 ... 905
UCST-1025 ... 905
UCST-1026 ... 905
UCST-1027 ... 906

Chapter 106 AUDIT ZONE System Messages

ZONE-3001 ... 908
ZONE-3002 ... 908
ZONE-3003 ... 909

ZONE-3004 909
ZONE-3005 910
ZONE-3006 910
ZONE-3007 910
ZONE-3008 911
ZONE-3009 911
ZONE-3010 911
ZONE-3011 912
ZONE-3012 912
ZONE-3013 912
ZONE-3014 913
ZONE-3015 913
ZONE-3016 914
ZONE-3017 914
ZONE-3018 914
ZONE-3019 915
ZONE-3020 915
ZONE-3021 916
ZONE-3022 916
ZONE-3023 916
ZONE-3024 917
ZONE-3025 917

Preface

As part of an effort to improve and enhance the performance and capabilities of its product lines, EMC periodically releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all versions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Audience

This document is part of the EMC Connectrix B Series Fabric OS 6.2 documentation set, and is intended for use by system administrators and technicians during installation and configuration of the switches to help you operate, maintain, and troubleshoot SAN products.

Readers of this document are expected to be familiar with the Fabric OS operating environment used on the EMC Connectrix B Series switches and directors.

Supported hardware and software

Although many different software and hardware configurations are tested and supported by EMC for Fabric OS v6.2, documenting all possible configurations and scenarios is beyond the scope of this document; however, this document does specify when procedures or parts of procedures apply only to specific switches.

This document does not support all Fabric OS versions. This document is specific to Fabric OS v6.2. To obtain information about a Fabric OS version other than v6.2, see the documentation specific to that OS version.

Related documentation

Related documents include:

- *EMC Connectrix B Series Fabric OS Encryption Administrator's Guide*
- *EMC Connectrix B Series Fabric OS Administrator's Guide*
- *EMC Connectrix B Series Fabric OS Command Reference Manual*
- *EMC Connectrix B Series Fabric OS Fabric Watch Administrator's Guide*
- *EMC Connectrix B Series Fabric OS MIB Reference Guide*
- *EMC Connectrix B Series Fabric OS Web Tools Administrator's Guide*
- *EMC Connectrix B Series Fabric OS Troubleshooting and Diagnostics Guide*

EMC Support Matrix

For the most up-to-date information, always consult the *EMC Support Matrix* (ESM), available through E-Lab Interoperability Navigator (ELN) at: http://elabnavigator.EMC.com, under the **PDFs and Guides** tab.

Conventions used in this document

EMC uses the following conventions for special notices.

Note: A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment.

IMPORTANT

An important notice contains information essential to operation of the software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the warning.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, utilities • URLs, pathnames, filenames, directory names, computer names, links, groups, service keys, file systems, notifications
Bold	Used in running (nonprocedural) text for: • Names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system call, man pages Used in procedures for: • Names of interface elements (such as names of windows, dialog boxes, buttons, fields, and menus) • What user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis (for example a new term) • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, filenames, prompts, and syntax when shown outside of running text
`Courier bold`	Used for: • Specific user input (such as commands)
`Courier italic`	Used in procedures for: • Variables on command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces indicate content that you must specify (that is, x or y or z)
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:

`http://Powerlink.EMC.com`

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Working with customer support

Contact the EMC Customer Support Center for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

- General information
  - Technical Support contract number, if applicable
  - Switch model
  - Switch operating system version
  - Error numbers and messages received
  - **supportSave** command output
  - Detailed description of the problem and specific questions
  - Description of any troubleshooting steps already performed and results
  - Serial console and telnet session logs
  - syslog message logs
- Switch Serial Number

  The switch serial number and corresponding bar code are provided on the serial number label, as shown here:

  FT00X0054E9
  `FT00X0054E9`

  The serial number label is located as follows:

  - *AP-7600B*—On the bottom of the chassis
  - *DS-220B*— Nonport side of the chassis

- *DS-300B, DS-4100B, DS-4900B, DS-5100B, DS-5300B, ES-5832B, and MP-7500B*—On the switch ID pull-out tab located inside the chassis on the port side on the left
- *ED-48000B*—Inside the chassis next to the power supply bays
- *DS-5000B*—On the switch ID pull-out tab located at the bottom of the port side of the switch.
- *ED-DCX-B and ED-DCX-4S-B*— On the bottom right on the port side of the chassis.

◆ World Wide Name (WWN) is obtained by providing the license ID. Use the **licenseIdShow** command to display the license ID.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to:

techpubcomments@EMC.com

1 Introduction to System Messages

This guide supports Fabric OS v6.2 and documents system messages that can help you diagnose and fix problems with a switch or fabric. The messages are organized first by event type, reliability, availability, and serviceability log (RASLog) or AUDIT, and then alphabetically by module name. A *module* is a subsystem in the Fabric OS. Each module generates a set of numbered messages. For each message, this guide provides message text, probable cause, recommended action, and severity level. There may be more than one cause and more than one recommended action for any given message. This guide discusses the most probable cause and typical action recommended.

This chapter provides an introduction to system messages. It includes the following topics:

- Overview of system messages 54
- Viewing and configuring system message logs..... 59
- Reading a RAS system message..... 65
- Responding to a system message 69
- System module descriptions 72

Overview of system messages

The Fabric OS maintains an internal system message log of all messages. All messages are tagged by type as either RASLog system error messages, Audit messages, or both. RASLog error messages are primarily designed to indicate and log abnormal, error-related events, whereas Audit messages record events such as login failures, zone, or configuration changes. Fabric OS supports a different methodology for storing and accessing each type of message.

This section provides information on the various logs saved by the system and how to view the information in the log files, including the following topics:

- System error message logging 54
- System logging daemon (syslogd) 57
- System console 58
- Port logs..... 58

System error message logging

The RASLog service generates and stores messages related to abnormal or erroneous system behavior. It includes the following features:

- All RASLog error messages are saved to nonvolatile storage by default.
- The system error message log can save a maximum of 1024 messages in random access memory (RAM).
- The system message log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are overwritten by new entries.
- Messages are numbered sequentially from 1 to 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
- By default, the **errDump** and **errShow** commands display all of the system error messages.

- Trace dump, first-time failure detection capture (FFDC), and core dump files can be uploaded to the FTP server using the **supportSave** command.
- It is recommended to configure the **syslogd** facility as a management tool for error logs. This is particularly important for dual-domain switches, as the **syslogd** facility saves messages from two logical switches as a single file and in sequential order. See "System logging daemon (syslogd)" on page 57 for more information.

Event auditing

Event auditing is designed to support post-event audits and problem determination based on high-frequency events of certain types such as security violations, zoning configuration changes, firmware downloads, and certain types of fabric events. Fabric OS versions earlier than v5.2.0 generated a subset of messages flagged as AUDIT in the RASLog to identify some of this type of output in addition to error log messages. In Fabric OS v5.2.0 and later, messages flagged as AUDIT are no longer saved in the switch's error logs. Instead, the switch can be configured to stream Audit messages to the switch console and to forward the messages to specified syslog server(s). There is no limit to the number of audit events.

For any given event, AUDIT messages capture the following information:

- User Name: The name of the user who triggered the action.
- User Role: For example, root or admin.
- Event Name: The name of the event that occurred.
- Status: The status of the event that occurred: success or failure.
- Event Info: Information about the event.

The five event classes listed in Table 1 can be audited:

Table 1 Event classes that can be audited

Operand	Event class	Description
1	Zone	You can audit zone event configuration changes, but not the actual values that were changed. For example, you may receive a message that states "Zone configuration has changed," but the message does not display the actual values that were changed.
2	Security	Security: You can audit any user-initiated security event for all management interfaces. For events that have an impact on the entire fabric, an audit is only generated for the switch from which the event was initiated.
3	Configuration	Configuration: You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
4	Firmware	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
5	Fabric	You can audit Administration Domain related changes.

Fabric OS v6.2 generates the following component-specific Audit messages:

- AG-related messages: AG 1029
- Authentication messages: AUTH 3001-3008
- Configuration messages: CONF-1000, 1020, 1022
- FCIP-related messages: FCIP 1002 and 1003
- FICU-related messages: FICU 1011 and 1012
- FW-related messages: FW - 3001
- HTTP configuration messages: HTTP-1002 - 1003
- IPAD-related messages: IPAD 1002
- PORT related messages: PORT 1006 - 1009
- SNMP related messages: SNMP-1004 - 1006
- Security related messages (RADIUS, login/logout, passwords, ACLs): SEC-3001 - 3041, 3044-3051
- Software upgrade library: SULB-1001 - 1004, 1009 - 1010, 1017 -1018, 1020 - 1021, 1023 - 1024, 1026, 1030 - 1035, 1037
- SWCH-related messages: SWCH 1012-1014
- UCST-related messages: UCST 1021-1024
- Zoning messages: ZONE-3001 - 3025

Event auditing is a configurable feature, set to off by default. You must enable event auditing by configuring the syslog daemon to send the events to a configured remote host using the **syslogIpAdd** command. You can set up filters to screen out particular classes of

events using the **auditCfg** command (the classes include zone, security, configuration, firmware, and fabric). The defined set of Audit messages are sent to the configured remote host in the Audit message format, so that they are easily distinguishable from other syslog events that might occur in the network. For details on how to configure event auditing, see "Viewing and configuring system message logs" on page 59.

System logging daemon (syslogd)

The system logging daemon (**syslogd**) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style **syslogd** process to forward system events and error messages to log files on a remote host system. The host system can be running UNIX, Linux, or any other operating system that supports the standard **syslogd** functionality. Configuring for **syslogd** involves configuring the host, enabling **syslogd** on the EMC® Connectrix® B Series model, and, optionally, setting the facility level.

For the enterpise-class platforms, each CP has a unique error log, depending on which CP was active when that message was reported. To fully understand message logging on these platforms you should enable the system logging daemon, because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as **firmwareDownload** or **haFailover**, for which the active CP changes.

For the enterpise-class platforms, security violations such as telnet, HTTP, and serial connection violations are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

For information on configuring **syslogd** functionality, refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide*.

System console

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you will not receive system console messages.

The system console displays system messages, Audit messages (if enabled) and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the system logs.

You can filter messages that appear on the system console by severity using the **errFilterSet** command. All messages are still sent to the system message log and syslog (if enabled).

Port logs

The Fabric OS maintains an internal log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

Run the **portLogShow** command to display the port logs for a particular port.

Run the **portLogEventShow** command to display the specific events reported for each port.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for information on interpreting results of the **portLogDump** command.

Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

Viewing and configuring system message logs

This section provides information on viewing and configuring system message logs, including:

- Viewing system messages from Web Tools 61
- Dumping system messages 61
- Viewing system messages from Web Tools 61
- Clearing the system message log 63
- Configuring event auditing 64

The procedures are valid for for all switches and enterprise-class platforms capable of running Fabric OS v6.0.x or higher.

Table 2 describes commands that you can use to view or configure the system message logs. Most commands require admin access level. For detailed information on required access levels and commands, refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual*.

Table 2 Commands for viewing or configuring the system parameters and logs (page 1 of 3)

Command	Description
agtCfgDefault	Resets the SNMP recipients to default values.
agtCfgSet	Modifies the SNMP agent configuration.
agtCfgShow	Displays the current SNMP agent configuration.
auditCfg	Configures the audit message log.
auditShow	Modifies and displays audit log filter configuration.
diagPost	Set or display diagnostic POST (Power-On Self-Test) configuration.
errClear	Clears all error log messages for all switch instances on this control processor (CP).
errDelimterSet	Sets the error log start and end delimiter for messages pushed to the console.
errDump	Displays the entire error log, without page breaks. Use the **-r** option to show the messages in reverse order, from newest to oldest.
errFilterSet	Sets an error severity filter for the system console.
errShow	Displays the entire error log, with page breaks. Use the **-r** option to show the messages in reverse order, from newest to oldest.

Table 2 Commands for viewing or configuring the system parameters and logs (page 2 of 3)

Command	Description
pdShow	Displays the contents of the panic dump and core dump files.
portErrShow	Displays the port error summary.
portLogClear	Clears the port log. If the port log is disabled, this commands enables it.
portLogDisable	Disables the port log facility.
portLogDump	Displays the port log, without page breaks.
portLogDumpPort	Displays the port log of the specified port, without page breaks.
portLogEventShow	Displays which port log events are currently being reported.
portLoginShow	Displays port logins.
portLogPdisc	Sets or clear the debug pdisc_flag.
portLogReset	Enables the port log facility.
portLogResize	Resizes the port log to the specified number of entries.
portLogShow	Displays the port log, with page breaks.
portLogShowPort	Displays the port log of specified port, with page breaks.
portLogTypeDisable	Disables an event from reporting to the port log. Port log events are described by the **portLogEventShow** command.
portLogTypeEnable	Enables an event to report to the port log. Port log events are described by the **portLogEventShow** command.
setVerbose	Sets the verbose level of a particular module within the Fabric OS.
supportFtp	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.
supportFfdc	Enables and disables FFDC (first failure data capture).
supportSave	Collects RASLog, trace files, and **supportShow** (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
supportShow	Executes a list of diagnostic and error display commands. This output is used by the EMC Customer Support Center to diagnose and correct problems with the switch. The output from this command is very long.
syslogDIpAdd	Adds an IP address as a recipient of system messages.
syslogDIpRemove	Removes an IP address as a recipient of system messages.

Table 2 **Commands for viewing or configuring the system parameters and logs (page 3 of 3)**

Command	Description
syslogDIpShow	Views the currently configured IP addresses that are recipients of system messages.
syslogdFacility	Changes the **syslogd** facility.
systemVerification	Use this command to run a comprehensive system wide test of all switches in a system. It will initiate a burnin run on all switches within the current system. Note that any reference seen to slot 0 is a reference to the blade within the switch platform, e.g., MP-7500B and AP-7600B contain PB-48K-18i and PB-48K-AP4-18 blades respectively.
traceDump	Displays, initiates, or removes a Fabric OS module trace dump.
traceTrig	Sets, removes, or displays trace triggers.

Viewing system messages from Web Tools

To view the system message log for a switch from Web Tools:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The **Switch View** displays.
3. Click the **Switch Events** tab from the **Switch Information Panel**. A **Switch Events Report** displays.
4. View the switch events and messages.

Dumping system messages

To display the system message log, with no page breaks:

1. Log in to the switch as admin.
2. Enter the **errDump** command at the command line:

```
Lab_DCX:admin> errdump
Fabric OS: v6.2.0a

2009/01/30-19:41:45, [SNMP-1005], 5, SLOT 7 | FID 128, INFO, Lab_DCX, SNMP
configuration attribute, Trap Severity Level 1 , has changed from 0 to 4

2009/01/30-20:35:48, [PLAT-1001], 17, SLOT 7 | CHASSIS, INFO, Lab_DCX, CP1
resetting other CP (double reset may occur).
```

```
2009/01/30-20:35:48, [HAMK-1004], 18, SLOT 7 | CHASSIS, INFO, Lab_DCX, Resetting
standby CP (double reset may occur)

2009/01/30-20:35:50, [ISNS-1011], 19, SLOT 7 | FID 128, INFO, Lab_DCX, iSNS Client
Service is disabled.

Lab_DCX:admin>
```

Viewing system messages one message at a time

To display the system message log one message at a time:

1. Log in to the switch as admin.
2. At the command line, enter the **errShow** command:

```
Lab_7500:admin> errshow
Fabric OS: v6.2.0a

2009/02/11-11:18:53, [BL-1030], 29792, CHASSIS, INFO, Lab_7500, All
GigE/FCIP/Virtualization/FC Fastwrite ports on the switch will be reset as part
of the firmware upgrade.

Type <CR> to continue, Q<CR> to stop:

2009/02/11-11:19:51, [IPAD-1000], 29793, CHASSIS, INFO, Lab_7500, SW/0 Ether/0
IPv6 autoconf 3ffe:80c0:22c:132:205:1eff:fe38:ff47/64 tentative DHCP Off

Type <CR> to continue, Q<CR> to stop:

2009/02/12-05:29:54, [SNMP-1005], 29832, FID 128, INFO, Lab_7500, SNMP
configuration attribute, Trap Severity Level 1 , has changed from 0 to 4

Type <CR> to continue, Q<CR> to stop:

2009/02/12-10:13:13, [SEC-1203], 29833, FID 128, INFO, Lab_7500, Login
information: Login successful via TELNET/SSH/RSH. IP Addr: 10.4.68.7

Type <CR> to continue, Q<CR> to stop:

2009/02/12-10:19:43, [SS-1000], 29835, CHASSIS, INFO, Lab_7500, supportSave has
uploaded support information to the host with IP address 10.4.68.7.

Type <CR> to continue, Q<CR> to stop:

Lab_7500:admin>
```

Clearing the system message log

To clear the system message log for a particular switch instance:

1. Log in to the switch as admin.
2. Use the **errClear** command to clear all messages from memory.

Note: For products that have a single processor, all error log messages are cleared. For products that have multiple processors, this command only clears the error logs of the processor it is executed from.

Configuring event auditing

To configure event auditing:

1. Configure the event classes you wish to audit:

```
switch:admin> auditcfg --class 1,2,3,4,5
Audit filter is configured.
```

2. Verify the configuration:

```
switch:admin> auditcfg --show
Audit filter is enabled.
1-ZONE
2-SECURITY
3-CONFIGURATION
4-FIRMWARE
5-FABRIC
```

3. Enable the audit feature:

```
switch:admin> auditcfg --enable
Audit filter is enabled.
```

4. Configure up to six syslog servers to receive the audit events that will be generated through syslog (procedure will vary depending on server type).
5. Configure syslog on the switch to point to the configured servers' IP addresses:

```
switch:admin> syslogdipadd 10.128.128.160
```

6. Verify the switch's syslog configuration:

```
switch:admin> syslogdipshow
syslog.1        192.168.163.234
syslog.2        10.128.128.160
```

Reading a RAS system message

This section provides information about reading system messages.

The following example shows the sample format of the RAS system error message:

```
<timestamp>, [<Event ID>], <Sequence Number>, <Flags>,<Severity>,<Switch name>,
<Event-specific information>
```

The following example shows a sample message from the error log:

```
2009/02/09-02:51:59, [UCST-1021], 79, SLOT 7 | FID 128, INFO, LAB_DCX, In-order
delivery option has been enabled
```

The fields in the message are described in Table 3:

Table 3 System message field description (page 1 of 2)

Example	Variable name	Description
2009/02/09-02:51:59	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized timestamp format base on the “LOCAL” setting.
[UCST-1021]	Message Module and Message Number	Displays the message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
79	Sequence Number	Represents the error message position in the log. When a new message is added to the log, this number is incremented by 1. When this message reaches the last position in the error log, and becomes the oldest message in the log, it is deleted when a new message is added. The message sequence number starts at 1 after a **firmwareDownload** and will increase up to a value of 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.

Table 3 System message field description (page 2 of 2)

Example	Variable name	Description
SLOT 7 | FID 128	SLOT *num* CHASSIS FID *num* AUDIT and/or FFDC Flags	For most messages, this field will contain CHASSIS, indicating the message is applicable to the chassis, or FID *num*, indicating it as a fabric message, where *num* represents the Fabric ID. Messages may contain the following additional values: SLOT *num*, indicating the slot number of the CP that the message applies to. In most cases, this will be the active CP. AUDIT indicates that this message is for a security issue. FFDC indicates that additional first failure data capture information has also been generated for this event. AUDIT:FFDC indicates that the message is for a security issue and additional FFDC information has been generated.
INFO	Severity Level	Displays the severity of the message in alpha format: 1 = Critical 2 = Error 3 = Warning 4 = Info
LAB_DCX	Switch name or chassis name, depending on the action; for example, high-availability (HA) messages typically show the chassis name, and login failures show the logical switch name.	This field displays the defined switch name or the chassis name of the switch. This value is truncated if it exceeds 16 characters in length. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.
In-order delivery option has been enabled	Message Description	This field displays a text string explaining the message encountered and providing parameters supplied by the software at runtime.

Audit event messages

Compared to RASLog messages, messages flagged as AUDIT provide additional user and system related information of interest for post event auditing and problem determination.

Audit event message format:

```
AUDIT, <timestamp>, [<Event ID>], <Severity>, <Event Class>, <User ID>/<Role>/<IP
address>/<Interface>/<app name>. <Admin Domain>/<Switch name>, <Reserved field
for future expansion>, <Event-specific information>
```

The following is a sample audit event message:

```
AUDIT, 2005/12/10-09:54:03, [SEC-1000], WARNING, SECURITY,
JohnSmith/root/192.168.132.10/Telnet/CLI, Domain A/JohnsSwitch, , Incorrect
password during login attempt.
```

The fields in the error message are described in Table 4.

Table 4 Audit message field description (page 1 of 2)

Example	Variable name	Description
AUDIT	Audit flag	Identifies the message as an Audit message.
2005/12/10-09:54:03	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized timestamp format base on the “LOCAL” setting.
[SEC-1000]	Message Module and Message Number	Displays the message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
WARNING	Severity Level	Displays the severity of the message in alpha format: 1 = Critical 2 = Error 3 = Warning 4 = Info
SECURITY	Event Class	Identifies the event class as one of the following: Zone Security Configuration Firmware Fabric
JohnSmith	User ID	Identifies the user ID.
root	Role	Identifies the role of the user ID.
192.168.132.10	IP Address	Identifies the IP address.
Telnet	Interface	Identifies the interface being used.
CLI	Application Name	Identifies the application name being used on the interface.
Domain A	Admin Domain	Identifies the Admin Domain, if there is one.

Table 4 Audit message field description (page 2 of 2)

Example	Variable name	Description
switchname	Switch name or chassis name, depending on the action; for example, HA messages typically show the chassis name and login failures show the logical switch name.	This field displays the defined switch name or the chassis name of the switch. This value is truncated if it is over 16 characters in length. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.
, ,	Null	Reserved for future use.
Slot 7 ejector not closed	Error Description	This field displays a text string explaining the error encountered and providing parameters supplied by the software at runtime.

Message severity levels

There are four levels of severity for messages, ranging from Critical (1) to Info (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you should look at each specific error message description thoroughly before taking action. System messages have the following severity levels.

1 = CRITICAL	Critical-level messages indicate that the software has detected serious problems that will cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
2 = ERROR	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = WARNING	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
4 = INFO	Info-level messages report the current non-error status of the system components: for example, detecting online and offline status of a fabric port.

Responding to a system message

This section provides procedures on gathering information on system messages, including:

- Looking up a system message 69
- Gathering information about the problem..... 69
- Support..... 70
- Panic dump and core dump files 70
- Trace dumps 71
- supportSave command 71

Looking up a system message

Error messages in this manual are arranged alphabetically. To look up an error message, copy down the module (see Table 5 on page 72) and the error code and compare this with the Table of Contents to determine the location of the information for that error message.

The following information is provided for each message:

- Module and code name for the error
- Message text
- Probable cause
- Recommended action
- Message severity

Gathering information about the problem

Common steps and questions to ask yourself when troubleshooting a system message are as follows:

1. What is the current Fabric OS level?
2. What is the switch hardware version?
3. Is the switch operational?
4. Assess impact and urgency:
    - Is the switch down?
    - Is it a standalone switch?
    - How large is the fabric?
    - Is the fabric redundant?

5. Run the **errDump** command on each logical switch.
6. Run **supportFtp** (as needed) to set up automatic FTP transfers, and then run the **supportSave** command.
7. Document the sequence of events by answering the following questions:
   - What happened just prior to the problem?
   - Is the problem repeatable?
   - If so, what are the steps to produce the problem?
   - What configuration was in place when the problem occurred?
8. Did a failover occur?
9. Was security enabled?
10. Was POST enabled?
11. Are serial port (console) logs available?
12. Which CP was master? (only applicable to the ED-DCX-B and the ED-48000B)
13. What and when were the last actions or changes made to the system?

Support

Fabric OS creates a number of files that can help EMC Customer Service troubleshoot and diagnose a problem This section describes those files and how to access and/or save the information for EMC Customer Service.

Panic dump and core dump files

The Fabric OS creates panic dump files and core files when there are problems in the Fabric OS kernel. You can view panic dump files using the **pdShow** command. These files can build up in the kernel partition (typically because of failovers) and might need to be periodically deleted or downloaded using the **supportSave** command.

The software watchdog process (SWD) is responsible for monitoring daemons critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a

predetermined interval defined for each daemon. The ping interval is set at 133 seconds, with the exception of the Fabric Watch daemon and the IP storage demon, which ping the SWD every 333 seconds. (For a complete listing of daemons, see Table 5, KSWD.)

If a daemon fails to ping the SWD within the defined interval, or if the daemon terminates unexpectedly, then the SWD dumps information to the panic dump files, which helps to diagnose the root cause of the unexpected failure.

Run the **pdShow** command to view these files or the **supportSave** command to send them to a host workstation using FTP. The panic dump files and core files are intended for EMC Customer Service use only.

Trace dumps

The Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. The Fabric OS trace dumps files are intended for EMC Customer Service use only. You can use the **supportSave** or **supportFTP** commands to collect trace dump files to a specified remote location to provide to EMC Customer Service when requested.

supportSave command

The **supportSave** command can be used to send the output of the system messages (RASLog), the trace files, and the output of the **supportShow** command to an off-switch storage location via FTP. Prior to running the **supportSave** command, you can optionally set up the FTP parameters using the **supportFtp** command. The **supportShow** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

System module descriptions

Table 5 provides a summary of the system modules for which messages are documented in this reference guide; the system modules are listed alphabetically by name.

Table 5 System module descriptions (page 1 of 7)

System module	Description
AG	Access Gateway allows multiple hosts (or HBAs) to access the fabric using fewer physical ports. Access Gateway mode transforms the DS-220B into a device management tool that is compatible with different types of fabrics, including Brocade/Connectrix B-, Cisco-, and McDATA-based fabrics.
AUTH	Authentication error messages indicate problems with the authentication module of the Fabric OS.
BKSW	Messages generated by the Blade Fabric OS kernel software watch dog module.
BL	Blade error messages are a result of faulty hardware, transient out-of-memory conditions, application specific integrated circuit (ASIC) errors, or inconsistencies in the software state between a blade and the EM (environment monitor) module.
BLL	Bloom is the name of the application specific integrated circuit (ASIC) used as the building block for third-generation hardware platforms.
BM	Blade management error messages are a result of autoleveling firmware upgrades performed by the control processor (CP).
C2	Condor2 application specific integrated circuit (ASIC) drive messages
CDR	Condor application specific integrated circuit (ASIC) driver error messages.
CER	This is the core edge routing module on the Connectrix B director platforms.
CHASSIS	Messages specific to the physical chassis.
CNM	Messages specific to encryption node management.
CONF	Status messages for **configUpload** and **configDownload** operations.
CTAP	Messages specific to encryption tape pools.
CLVC	Messages specific to encryption LUNs.
CLVM	Messages specific to the encryption modules.

Table 5 System module descriptions (page 2 of 7)

System module	Description
EM	The environmental monitor (EM) manages and monitors the various field replaceable units (FRUs), including the port cards, control processor (CP) blades, blower assemblies, power supplies, and world-wide name (WWN) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery. EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status by way of CLI commands, system light emitting diodes (LEDs), and status and alarm messages. EM also manages some component-related data.
ESS	Messages specific to Coordinated Hot Code Load.
EVMD	This is the event management module.
FABR	FABRIC refers to a network of Fibre Channel switches. The FABRIC error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FBC	Firmware blade compatibility errors with control processor (CP).
FCIP	Fibre Channel over IP port configuration messages.
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
FCR	Fibre Channel router related traffic and activity on the fabric or backend fabric.
FICN	Messages specific to FICON.
FICU	The FICON-CUP daemon handles communication with fibre connectivity (FICON) on IBM FICON storage devices. Errors to this module are usually initiation errors or indications that FICON-CUP prerequisites have not been met, such as a license key, core process ID (PID), and secure mode on the fabric.
FKLB	Fabric OS I/O kernel library module.
FLOD	FLOD is a part of the fabric shortest path first (FSPF) protocol that handles synchronization of the link state database (LSDB) and propagation of the link state records (LSRs).
FSPF	Fabric shortest path first (FSPF) is a link state routing protocol that is used to determine how frames should be routed. These messages are about protocol errors.

Table 5 System module descriptions (page 3 of 7)

System module	Description
FSS	The Fabric OS state synchronization framework provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take control of the switch nondisruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation. FSS is defined both as a component and a service. A *component* is a module in the Fabric OS, implementing a related set of functionality. A *service* is a collection of components grouped together to achieve a modular software architecture.
FSSM	The Fabric OS state synchronization management module is defined both as a component and a service. A component is a module in Fabric OS implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.
FW	FW is the Fabric Watch module. This module monitors thresholds for many switch subsystems: for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.
HAM	HAM is a user space daemon responsible for high availability management.
HAMK	This is the kernel module for the high availability management (HAM) daemon.
HIL	Hardware independent layer.
HLO	HLO is a part of the fabric shortest path first (FSPF) protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.
HMON	Health monitor.
HTTP	HTTP error messages.
IBD	This raslog generates messages related to port restart failure.
IBPD	IBPD stands for iSCSI gateway daemon on a blade processor (BP). It manages iSCSI initiator access control, session authentication, and session/connection statistics.
ICPD	ICPD stands for iSCSI gateway daemon on a control processor (CP). It manages iSCSI configurations such as CHAP, VT/LUN, DD/DDSet and portal configurations, and statistics such as iSCSI session/connection information. Moreover, ICPD distributes iSCSI configurations not only switch wide, but also fabric wide. It keeps track iSCSI VT status and updates VT status to BP.
IPAD	System messages generated by the IP admin demon.
IPS	Fibre Channel over IP license, tunneling, and port related messages.
ISCS	The ISCS module is the FabOS component that performs system-level control of the iSCSI Gateways. Its functions include: initialization, message delivery from iSCSI protocol clients, system error monitoring, and fault recovery.
ISNS	ISNS server and client status messages.

Table 5 System module descriptions (page 4 of 7)

System module	Description
KAC	Message specific to the encryption key archive client.
KSWD	The kernel software watchdog (KSWD) watches daemons for unexpected terminations and "hang" conditions and informs the HAM module to take corrective actions such as failover or reboot. The following daemons are monitored by KSWD: • Access Gateway daemon (agd) • Alias Server (asd) • ARR daemon (arrd) • Authentication daemon (authd) • Blade Manager (bmd) • Common Access Layer (cald) • Diagnostics daemon (diagd) • Environment Monitor (emd) • EVM daemon (evmd) • Exchange Service Support daemon (essd) • FA-API rpc daemon (rpcd) • Fabric daemon (fabricd) • Fabric Watch daemon (fwd) • FCPD daemon (fcpd) • FDMI daemon (fdmid) • FICON CUP daemon (ficud) • FSPF daemon (fspfd) • Inter-fabric Routing daemon (iswitchd) • IP Storage Daemon (ipsd) • iSCSI daemon on CP (icpd) • iSNS client daemon on CP (isnscd) • Management Server daemon (msd) • Name Server Daemon (nsd) • PDM daemon (pdmd) • PS daemon (psd) • RASLOG daemon (raslogd) • RSC daemon (rcsd) • SAS CP Daemon (scpd) • Security daemon (secd) • SNMP daemon (snmpd) • Time Service daemon (tsd) • TRACE daemon (traced) • Track Changes daemon (trackd) • Web tools daemon (webd)

Table 5 System module descriptions (page 5 of 7)

System module	Description
KTRC	Kernel RAS trace module.
LFM	Messages specific to the Logical Fabric Manager.
LOG	RASLog subsystem.
LSDB	The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.
MFIC	MS-FICON messages relate to fibre connectivity (FICON) installations. Fibre connectivity control unit port (FICON-CUP) messages are displayed under the FICU module.
MPTH	Multicast path uses the shortest path first (SPF) algorithm to dynamically compute a broadcast tree.
MQ	Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or interrupt service routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	The Management Service enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas: **Fabric Configuration Server**. Provides for the configuration management of the fabric. **Unzoned Name Server**. Provides access to Name Server information that is not subject to zone constraints. **Fabric Zone Server**. Provides access to and control of zone information.
NBFS	NBFSM is a part of the fabric shortest path first (FSPF) protocol that handles a neighboring or adjacent switch's finite state machine (FSM). Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an ISL (interswitch link) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on. NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).
NS	Indicates problems with the simple name server module.
PDM	Parity data manager is a user space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	These messages indicate panic dump trace files have been created.
PLAT	This message indicates hardware problems.
PMGR	Messages specific to switch Fabric IDs.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users, to connect end devices or connect to other switches.

Table 5 System module descriptions (page 6 of 7)

System module	Description
PS	The performance server daemon measures the amount of traffic between end points or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.
PSWP	The portswap feature and associated commands generate these error messages.
RAS	First failure data capture (FFDC), informational message when FFDC events are logged to the FFDC log and size/roll over warning.
RCS	The reliable commit service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests reliable transport write and read (RTWR) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RKD	Messages specific to encryption key/rekey operations.
RPCD	The remote procedure call daemon (RPCD) is used by Fabric Access for API-related tasks.
RTWR	The reliable transport write and read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an “unreachable” message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SAS	Storage application services supporting director-class storage virtualization platform.
SCN	The internal state change notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages, to distinguish between internal switch and fabric operation errors, and external attack.
SNMP	Simple Network Management Protocol is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Connectrix B switches support six management entities that can be configured to receive these traps.
SPC	Messages specific to the crypto hardware.
SPM	Messages specific to the crypto certificates and key vault.
SS	The **supportSave** command generates these error messages if problems are encountered.
SULB	The software upgrade library provides **firmwareDownload** command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondisruptive code load to all 4.x switches. These messages might display if there are any problems during the **firmwareDownload** procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide*.

Table 5 System module descriptions (page 7 of 7)

System module	Description
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
SYSM	General system messages.
TAPE	Messages specific to tape pools.
TRCE	RAS TRACE error messages.
TRCK	The track change feature tracks the following events: Turning on or off the track change feature CONFIG_CHANGE LOGIN LOGOUT FAILED_LOGIN If any of these events occurs, a message is sent to the system message log. Additionally, if the SNMP trap option is enabled, an SNMP trap is also sent. For information on configuring the track change feature, refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* or the *EMC Connectrix B Series Fabric OS Administrator's Guide*.
TS	Time Service provides fabric time-synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.
UCST	UCAST is a part of the fabric shortest path first (FSPF) protocol that manages the Unicast routing table.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a Unicast tree.
WEBD	Indicates problems with the Web Tools module.
ZOLB	Indicates problems with the zone library module.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

Note: Any reference seen in a system message to slot 0 is a reference to the blade within the switch platform, for example: the ED-DCX-B can contain PB-DCX-48P and PB-DCX-16P blades

PART 1

RASLog Messages

This section provides the RASLog messages.

For a list of these messages, refer to the Table of Contents on page 3.

2

AG System Messages

This chapter contains information on the following AG messages:

- AG-1001 83
- AG-1002 83
- AG-1003 84
- AG-1004 84
- AG-1005 84
- AG-1006 85
- AG-1007 85
- AG-1008 85
- AG-1009 86
- AG-1010 86
- AG-1011 86
- AG-1012 87
- AG-1013 87
- AG-1014 88
- AG-1015 88
- AG-1016 88
- AG-1017 89
- AG-1018 89
- AG-1019 89
- AG-1020 90
- AG-1021 90
- AG-1022 90
- AG-1023 91
- AG-1024 91
- AG-1025 92
- AG-1026 92
- AG-1027 93
- AG-1028 93

◆ AG-1029 93

AG-1001

Message

```
<timestamp>, [AG-1001], <sequence-number>,, ERROR,
<system-name>, N_Port ID virtualization (NPIV) is not
supported by fabric port connected to port <port>.
```

Probable cause

N_Port ID virtualization (NPIV) capability is not supported by the fabric port to which the Access Gateway is connected.

Recommended action

- On switches running Fabric OS 6.0 or earlier versions, run the **portCfgNpivPort** command to enable NPIV capability on the port connected to the Access Gateway. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on this command.
- Some blades or ports in a switch may not have support for NPIV. NPIV functionality cannot be enabled on such ports and they will not respond to NPIV requests. Refer to the *EMC Connectrix B Series Fabric OS Access Gateway Administrator's Guide,* Appendix B, for specific AG compatibility requirements.
- On non-Connectrix B switches, refer to the manufacture's documentation to determine whether the switch supports NPIV and how to enable NPIV on these types of switches.

Severity

ERROR

AG-1002

Message

```
<timestamp>, [AG-1002], <sequence-number>,, WARNING,
<system-name>, Unable to find alternate N_Port during
failover for N_Port <port>.
```

Probable cause

No other N_Port is configured or the fabric was unstable during failover.

Recommended action

Check whether or not an alternate N_Port is configured.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

AG-1003

Message

```
<timestamp>, [AG-1003], <sequence-number>,, WARNING,
<system-name>, Unable to failover N_Port <port>. Failover
across different fabrics is not supported.
```

Probable cause

Failover across N_Ports connected to different fabrics is not supported.

Recommended action

Configure two or more N_Ports to connect to the same fabric; then execute **ag --failoverEnable** to enable failover on these N_Ports.

Severity

WARNING

AG-1004

Message

```
<timestamp>, [AG-1004], <sequence-number>,, ERROR,
<system-name>, Invalid response to fabric login (FLOGI)
request from the fabric for N_Port <port>.
```

Probable cause

Indicates that the fabric sent an invalid response to the FLOGI Extended Link Service (ELS) for the specified N_Port.

Recommended action

Check the configuration of the fabric switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AG-1005

Message

```
<timestamp>, [AG-1005], <sequence-number>,, WARNING,
<system-name>, FDISC response was dropped because F_Port
<port> is offline.
```

Probable cause

Indicates that the F_Port connected to the host is offline, which caused the FDISC response to drop.

Recommended action

Check the configuration of the host connected to the specified F_Port.

Severity WARNING

AG-1006

Message `<timestamp>, [AG-1006], <sequence-number>,, INFO, <system-name>, Access Gateway mode has been <msg>.`

Probable cause Access Gateway mode has been enabled or disabled.

Recommended action Run **ag --modeShow** to verify the current status of the Access Gateway mode.

Severity INFO

AG-1007

Message `<timestamp>, [AG-1007], <sequence-number>,, WARNING, <system-name>, FLOGI response not received for the N_Port <port> connected to the fabric.`

Probable cause Indicates that the N_Port connected to the fabric switch is not online. The specified N_Port has been disabled.

Recommended action Check the connectivity between the Access Gateway N_Port and the fabric switch port.

Severity WARNING

AG-1008

Message `<timestamp>, [AG-1008], <sequence-number>,, WARNING, <system-name>, Invalid port login (PLOGI) response from the fabric on the N_Port <port>.`

Probable cause Indicates that the fabric switch management server did not accept the N_Port Login (PLOGI) request sent by the Access Gateway.

Recommended action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AG-1009

Message `<timestamp>, [AG-1009], <sequence-number>,, WARNING, <system-name>, Sending FLOGI failed on N_Port <port>.`

Probable cause Failure sending a Fabric Login (FLOGI) request from the Access Gateway to the fabric switch.

Recommended action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AG-1010

Message `<timestamp>, [AG-1010], <sequence-number>,, WARNING, <system-name>, Sending PLOGI failed on N_Port <port>.`

Probable cause Failure sending an N_Port Login (PLOGI) request from the Access Gateway to the fabric switch.

Recommended action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AG-1011

Message `<timestamp>, [AG-1011], <sequence-number>,, WARNING, <system-name>, Sending FDISC failed on N_Port <port>.`

Probable cause Indicates there was a failure sending the discover F_Port service parameter request from the Access Gateway to the fabric switch.

Recommended action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AG-1012

Message

```
<timestamp>, [AG-1012], <sequence-number>,, WARNING,
<system-name>, Sending logout(LOGO)request failed on
N_Port <port>.
```

Probable cause Failure sending an N_Port logout request from the Access Gateway to the fabric switch.

Recommended action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AG-1013

Message

```
<timestamp>, [AG-1013], <sequence-number>,, INFO,
<system-name>, F_Ports mapped to N_Port <port> failed
over to other N_Port(s).
```

Probable cause Indicates that the specified N_Port is failing over to other N_Port(s) connected to the same fabric.

Recommended action Run the **ag --mapShow** command to display updated F_Port to N_Port mappings.

Severity INFO

AG-1014

Message

```
<timestamp>, [AG-1014], <sequence-number>,, INFO,
<system-name>, Failing back F_Ports mapped to N_Port
<port>.
```

Probable cause

Indicates that the specified N_Port is failing back F_Ports mapped to the specified N_Port.

Recommended action

Run the **ag --mapShow** command to display updated F_Port to N_Port mappings.

Severity

INFO

AG-1015

Message

```
<timestamp>, [AG-1015], <sequence-number>,, WARNING,
<system-name>, Unable to find online N_Ports to connect
to the fabric.
```

Probable cause

Either no other N_Port is configured or all N_Ports are currently offline.

Recommended action

Check whether or not any other N_Port is configured.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

AG-1016

Message

```
<timestamp>, [AG-1016], <sequence-number>,, INFO,
<system-name>, Failing over F_Ports mapped to N_Port
<port> to other N_Port(s).
```

Probable cause

Indicates that the specified N_Port has failed to come online. All F_Port(s) mapped to this N_Port are being failed over to other active N_Port(s).

Recommended action

Run the **ag --mapShow** command to display updated F_Port to N_Port mappings.

Severity INFO

AG-1017

Message
```
<timestamp>, [AG-1017], <sequence-number>,, WARNING,
<system-name>, No N_Port(s) are currently Online.
```

Probable cause Indicates that no N_Port(s) are currently configured in the system or all configured N_Port(s) have failed to come online.

Recommended action Run **switchShow** to display the status of all ports in the system. Run **portCfgShow** to display a list of ports currently configured as N_Port(s).

Severity WARNING

AG-1018

Message
```
<timestamp>, [AG-1018], <sequence-number>,, ERROR,
<system-name>, Host port should not be connected to port
<port>, which is configured as N_Port.
```

Probable cause Indicates that Initiator/Target is erroneously connected to a port configured for N_Port operation.

Recommended action Run **switchShow** to display the status of all ports in the system. Run **portCfgShow** to display a list of ports currently configured as N_Port(s). Ensure that the host is connected to an F_port.

Severity ERROR

AG-1019

Message
```
<timestamp>, [AG-1019], <sequence-number>,, WARNING,
<system-name>, Unable to failover N_Port <port>. No other
N Port in port group:<pgid> is online.
```

Probable Cause Failover across port groups is not supported.

Recommended action Check whether or not an alternate N_Port is configured in this port group.

Severity WARNING

AG-1020

Message

```
<timestamp>, [AG-1020], <sequence-number>,, INFO,
<system-name>, F_Ports to N_Ports route/mapping has
been changed.
```

Probable Cause

Indicates that F_Port to N_Port mapping has been changed because the switch has come online or some new N_Port/F_Port has come online.

Recommended action

Run the **ag --mapshow** command to display the updated F_Port to N_Port mappings.

Severity

INFO

AG-1021

Message

```
<timestamp>, [AG-1021], <sequence-number>,, WARNING,
<system-name>, Unable to do Preferred-Failover of F_Port
<port>. Failover across different fabric is not
supported.
```

Probable Cause

Failover across N_Ports connected to different fabrics is not supported.

Recommended action

Change the preferred N_Port settings for this F_Port using **ag--prefset**.

Choose the preferred N_Port such that it is in the same fabric as the primary N_Port of this F_Port. Use **ag --show** to check the fabric connectivity of N_Ports.

Severity

WARNING

AG-1022

Message

```
<timestamp>, [AG-1022], <sequence-number>,, INFO,
<system-name>, F_Port <fport> is failed over to its
preferred N_Port <nport>.
```

Probable Cause

Indicates that the specified F_Port is failing over to its preferred N_Port.

Recommended action Run the **ag --mapshow** command to display updated F_Port to N_Port mappings.

Severity INFO

AG-1023

Message

```
<timestamp>, [AG-1023], <sequence-number>,, INFO,
<system-name>, F_Port <fport> mapped to offline N_Port
<nport> is failed over to its preferred N_Port <pport>.
```

Probable Cause Indicates that the specified N_Port has failed to come online. The F_Port mapped to this N_Port had its preferred set and is online.

Recommended action Run the **ag --mapshow** command to display updated F_Port to N_Port mappings.

Severity INFO

AG-1024

Message

```
<timestamp>, [AG-1024], <sequence-number>,, INFO,
<system-name>, F_Port <fport> is failed back to its
preferred N_Port <nport>.
```

Probable Cause Indicates that the specified N_Port is failing back F_Ports, which are failed over to some other N_Port.

Recommended action Run the **ag --mapshow** command to display the updated F_Port to N_Port mappings.

Severity INFO

AG-1025

Message

```
<timestamp>, [AG-1025], <sequence-number>,, ERROR,
<system-name>, Port group of Slave N_Port <port> is
different than its Master N_Port <m_port>.
```

Probable Cause

Indicates that the port group of Master and Slave N_Ports are different while the Trunk Area assigned to the attached F_Ports on edge switch is the same.

Recommended Action

Run the **porttrunkarea --show** command on the attached switch to display that the Trunk Area is assigned to all ports in the system and run **porttrunkarea --enable** to reconfigure the Trunk Area.

Severity

ERROR

AG-1026

Message

```
<timestamp>, [AG-1026], <sequence-number>,, WARNING,
<system-name>, Unable to handle the login request on port
<port> due to insufficient resources.
```

Probable Cause

Insufficient resources.

Recommended Action

Run the **configure** command on the Access Gateway switch and increase the number of allowed logins on this port.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

AG-1027

Message

```
<timestamp>, [AG-1027], <sequence-number>,, WARNING,
<system-name>, Unable to handle this login request on
port <port> because NPIV capability is not enabled on
this port.
```

Probable Cause NPIV is not enabled.

Recommended Action Run the **portcfgnpivport** command on Access Gateway switch and enable the NPIV capability on this port.

Severity WARNING

AG-1028

Message

```
<timestamp>, [AG-1028], <sequence-number>,, WARNING,
<system-name>, Device with Port WWN <port_name> tried to
perform fabric login through port <fport>, without having
access permission.
```

Probable Cause The device does not have access to login as per the ADS policy set by the user for that port.

Recommended Action Add the device in to the ADS allow list for that port using **ag --adsadd** command.

Severity WARNING

AG-1029

Message

```
<timestamp>, [AG-1029], <sequence-number>,, INFO,
<system-name>, F_Port to N_Port mapping has been updated
for N_Port <n_port>.
```

Probable Cause Indicates that the F_Ports mapped to an N_Port have changed and the config file has been updated.

Recommended Action No action is required.

Severity INFO

3

AUTH System Messages

This chapter contains information on the following AUTH messages:

- AUTH-1001 97
- AUTH-1002 97
- AUTH-1003 97
- AUTH-1004 98
- AUTH-1005 98
- AUTH-1006 99
- AUTH-1007 99
- AUTH-1008 99
- AUTH-1010 100
- AUTH-1011 100
- AUTH-1012 100
- AUTH-1013 101
- AUTH-1014 101
- AUTH-1016 102
- AUTH-1017 102
- AUTH-1018 102
- AUTH-1020 103
- AUTH-1022 103
- AUTH-1023 104
- AUTH-1025 105
- AUTH-1026 105
- AUTH-1027 106
- AUTH-1028 106
- AUTH-1029 107
- AUTH-1030 107
- AUTH-1031 108
- AUTH-1032 108

- AUTH-1033 109
- AUTH-1034 109
- AUTH-1035 109
- AUTH-1036 110
- AUTH-1037 110
- AUTH-1038 111
- AUTH-1039 111
- AUTH-1040 112
- AUTH-1041 112
- AUTH-1042 113
- AUTH-1043 113
- AUTH-1044 113

AUTH-1001

Message

```
<timestamp>, [AUTH-1001], <sequence-number>,, INFO,
<system-name>, <Operation type> has been successfully
completed.
```

Probable cause

Indicates that the secret database operation has been updated using the **secAuthSecret** command. The values for *Operation type* can be "set" or "remove".

Recommended action

No action is required.

Severity

INFO

AUTH-1002

Message

```
<timestamp>, [AUTH-1002], <sequence-number>,, ERROR,
<system-name>, <Operation type> has failed.
```

Probable cause

Indicates that the specified action has failed to update the secret database using the **secAuthSecret** command. The values for *Operation type* can be "set" or "remove".

Recommended action

Retry the **secAuthSecret** command.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1003

Message

```
<timestamp>, [AUTH-1003], <sequence-number>,, INFO,
<system-name>, <data type> type has been successfully set
to <setting value>.
```

Probable cause

Indicates that an authentication configuration value was set to the specified value. The *data type* is either "authentication type", "DH group type", or "policy type".

Recommended action No action is required.

Severity INFO

AUTH-1004

Message `<timestamp>, [AUTH-1004], <sequence-number>,, ERROR, <system-name>, Failed to set <data type> type to <setting value>.`

Probable cause Indicates that the **authUtil** command has failed to set the authentication configuration value. The *data type* is either "authentication type", "DH group type", or "policy type".

Recommended action Retry the **authUtil** command.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1005

Message `<timestamp>, [AUTH-1005], <sequence-number>,, ERROR, <system-name>, Authentication file does not exist: <error code>.`

Probable cause Indicates an authentication file corruption.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1006

Message

```
<timestamp>, [AUTH-1006], <sequence-number>,, WARNING,
<system-name>, Failed to open authentication
configuration file.
```

Probable cause

Indicates an internal problem with the Secure Fabric OS.

Recommended action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

AUTH-1007

Message

```
<timestamp>, [AUTH-1007], <sequence-number>,, ERROR,
<system-name>, The proposed authentication protocol(s)
are not supported: port <port number>.
```

Probable cause

Indicates that the proposed authentication protocol type or types are not supported by the local specified port.

Recommended action

Run the **authUtil** command to make sure the local switch supports the specified protocols: Fibre channel authentication protocol (FCAP) or Diffie Hellman - challenge handshake authentication protocol (DH-CHAP).

Severity

ERROR

AUTH-1008

Message

```
<timestamp>, [AUTH-1008], <sequence-number>,, ERROR,
<system-name>, No security license, operation failed.
```

Probable cause

Indicates that the switch does not have a security license.

Recommended action

Verify that the security license is installed using the **licenseShow** command. If necessary, reinstall the license using the **licenseAdd** command.

Severity ERROR

AUTH-1010

Message `<timestamp>, [AUTH-1010], <sequence-number>,, ERROR, <system-name>, Failed to initialize security policy: switch <switch number>, error <error code>.`

Probable cause Indicates an internal problem with the Secure Fabric OS.

Recommended action Reboot or power cycle the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1011

Message `<timestamp>, [AUTH-1011], <sequence-number>,, WARNING, <system-name>, Failed to register for failover operation: switch <switch number> error <error code>.`

Probable cause Indicates an internal problem with the Secure Fabric OS.

Recommended action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AUTH-1012

Message `<timestamp>, [AUTH-1012], <sequence-number>,, WARNING, <system-name>, Authentication <code> is rejected: port <port number> explain <explain code> reason <reason code>.`

Probable cause Indicates that an authentication is rejected because the remote entity does not support authentication.

Recommended action Make sure the entity at the other end of the link supports authentication.

Severity WARNING

AUTH-1013

Message

```
<timestamp>, [AUTH-1013], <sequence-number>,, WARNING,
<system-name>, Can not perform authentication request
message: port <port number>, message code <message code>.
```

Probable cause Indicates that the system is running low on resources when receiving an authentication request.

Recommended action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

AUTH-1014

Message

```
<timestamp>, [AUTH-1014], <sequence-number>, FFDC, ERROR,
<system-name>, Invalid port value to <operation>: port
<port number>.
```

Probable cause Indicates an internal problem with the Secure Fabric OS.

Recommended action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1016

Message `<timestamp>, [AUTH-1016], <sequence-number>, FFDC, ERROR, <system-name>, Invalid value to start HBA authentication port: <port number>, <pid>.`

Probable cause Indicates an internal problem.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1017

Message `<timestamp>, [AUTH-1017], <sequence-number>,, ERROR, <system-name>, Invalid value to start authentication request: port <port number>, operation code <operation code>.`

Probable cause Indicates an internal problem with the Secure Fabric OS.

Recommended action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1018

Message `<timestamp>, [AUTH-1018], <sequence-number>,, ERROR, <system-name>, Invalid value to check protocol type: port <port number>.`

Probable cause Indicates an internal problem with the Secure Fabric OS.

Recommended action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1020

Message

```
<timestamp>, [AUTH-1020], <sequence-number>,, INFO,
<system-name>, Failed to create timer for authentication:
port <port number>.
```

Probable cause Indicates that an authentication message's timer was not created.

Recommended action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

AUTH-1022

Message

```
<timestamp>, [AUTH-1022], <sequence-number>,, ERROR,
<system-name>, Failed to extract <data type> from
<message> payload: port <port number>.
```

Probable cause Indicates that the authentication process failed to extract a particular value from the receiving payload.

Recommended action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1023

Message

```
<timestamp>, [AUTH-1023], <sequence-number>,, ERROR,
<system-name>, Failed to <operation type> during
<authentication phase>: port <port number>.
```

Probable cause

Indicates an authentication operation failed for a certain authentication phase.

Operation type varies depending on authentication type:

- Some operations for switch link authentication protocol (SLAP): certificate retrieve, certificate verification signature verification, or nonce signing.
- Some operations for fibre channel authentication protocol (FCAP): certificate retrieve, certificate verification, signature verification, or nonce singing.
- Some operations for Diffie Hellman - challenge handshake authentication Protocol (DH-CHAP). response calculation, challenge generation, or secret retrieve.

The *authentication phase* specifies which phase of a particular authentication protocol failed.

A *nonce* is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended action

The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for possible unauthorized access attack.

It might indicate that the public key infrastructure (PKI) object for SLAP or FCAP or secret value for DH-CHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DH-CHAP properly.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1025

Message

```
<timestamp>, [AUTH-1025], <sequence-number>,, ERROR,
<system-name>, Failed to get <data type> during
<authentication phase>: port <port number>.
```

Probable cause

Indicates that the authentication process failed to get the expected information during the specified authentication phase.

Recommended action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1026

Message

```
<timestamp>, [AUTH-1026], <sequence-number>,, WARNING,
<system-name>, Failed to get <Device information> during
negotiation phase: port <port number>.
```

Probable cause

Indicates that the authentication failed to get device or host bus adaptor (HBA) information due to an internal failure.

Recommended action

Usually this problem is transient. If the authentication failed, retry the login.

Reinitialize authentication using the **switchDisable** and **switchEnable** commands or the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

AUTH-1027

Message

```
<timestamp>, [AUTH-1027], <sequence-number>,, ERROR,
<system-name>, Failed to select <authentication value>
during <authentication phase>: value <value> port <port
number>.
```

Probable cause

Indicates that the authentication process failed to select an *authentication value* (that is, DH Group, hash value, or protocol type) from a receiving payload for the specified *authentication phase*. This indicates that the local switch does not support the specified authentication value.

Recommended action

Check the authentication configuration and reset the supported value if needed using the **authUtil** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1028

Message

```
<timestamp>, [AUTH-1028], <sequence-number>,, ERROR,
<system-name>, Failed to allocate <data type> for
<operation phase>: port <port number>.
```

Probable cause

Indicates that the authentication process failed because the system is low on memory.

Data type is the payload or structure that failed to get memory. *Operation phase* specifies which operation of a particular authentication phase failed.

Recommended action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1029

Message

```
<timestamp>, [AUTH-1029], <sequence-number>,, ERROR,
<system-name>, Failed to get <data type> for <message
phase> message: port <port number>, retval <error code>.
```

Probable cause Indicates that the authentication process failed to get a particular authentication value at certain phase.

Data type is the payload or structure that failed to get memory.

Recommended action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1030

Message

```
<timestamp>, [AUTH-1030], <sequence-number>,, ERROR,
<system-name>, Invalid message code for <message phase>
message: port <port number>.
```

Probable cause Indicates the receiving payload does not have valid message code for a particular authentication phase.

Recommended action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1031

Message `<timestamp>, [AUTH-1031], <sequence-number>,, ERROR, <system-name>, Failed to retrieve secret value: port <port number>.`

Probable cause Indicates that the secret value was not set properly for the authenticated entity.

Recommended action Reset the secret value by using **secAuthSecret** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

Severity ERROR

AUTH-1032

Message `<timestamp>, [AUTH-1032], <sequence-number>,, ERROR, <system-name>, Failed to generate <data type> for <message payload> payload: length <data length>, error code <error code>, port <port number>.`

Probable cause Indicates that the authentication process failed to generate specific data (that is, challenge, nonce, or response data) for an authentication payload. This usually relates to internal failure.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1033

Message

```
<timestamp>, [AUTH-1033], <sequence-number>,, ERROR,
<system-name>, Disable port <port number> due to
unauthorized switch <switch WWN value>.
```

Probable cause

Indicates that an entity was not configured in the switch connection control (SCC) policy and tried to connect to the port.

Recommended action

Add the entity's world-wide name (WWN) to the SCC policy and reinitialize authentication by using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

Severity

ERROR

AUTH-1034

Message

```
<timestamp>, [AUTH-1034], <sequence-number>,, ERROR,
<system-name>, Failed to validate name <entity name> in
<authentication message>: port <port number>.
```

Probable cause

Indicates that the specified entity name in the payload is not in the correct format.

Recommended action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1035

Message

```
<timestamp>, [AUTH-1035], <sequence-number>,, ERROR,
<system-name>, Invalid <data type> length in <message
phase> message: length <data length>, port <port number>.
```

Probable cause

Indicates that a particular data field in the authentication message has an invalid length field. This error usually relates to internal failure.

Recommended action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1036

Message

```
<timestamp>, [AUTH-1036], <sequence-number>,, ERROR,
<system-name>, Invalid state <state value> for
<authentication phase>: port <port number>.
```

Probable cause

Indicates that the switch received an unexpected authentication message.

Recommended action

Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1037

Message

```
<timestamp>, [AUTH-1037], <sequence-number>,, ERROR,
<system-name>, Failed to <operation type> response for
<authentication message>: init_len <data length>,
resp_len <data length>, port <port number>.
```

Probable cause

Indicates that a Diffie Hellman - challenge handshake authentication protocol (DH-CHAP) authentication operation failed on the specified port due to mismatched response values between two entities.

Recommended action

The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1038

Message

```
<timestamp>, [AUTH-1038], <sequence-number>,, ERROR,
<system-name>, Failed to retrieve certificate during
<authentication phase>: port <port number>.
```

Probable cause Indicates that the public key infrastructure (PKI) certificate is not installed properly.

Recommended action Reinstall the PKI certificate, using the **pkiCreate** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1039

Message

```
<timestamp>, [AUTH-1039], <sequence-number>,, ERROR,
<system-name>, Neighboring switch has conflicting
authentication policy: Port <Port Number> disabled.
```

Probable cause Indicates that the neighboring switch has a conflicting authentication policy enabled. The E_Port has been disabled, because the neighboring switch rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended action Correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port using the **portEnable** command.

Severity ERROR

AUTH-1040

Message `<timestamp>, [AUTH-1040], <sequence-number>,, INFO, <system-name>, Reject authentication on port <Port Number>, because switch authentication policy is set to OFF.`

Probable cause Indicates that the local switch has rejected the authentication because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the light will go off due to conflicting configuration settings. Otherwise the E_Port will form without authentication.

Recommended action If there is no light on the port, correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port on the neighboring switch using the **portEnable** command. If the E_Port formed, no action is required.

Severity INFO

AUTH-1041

Message `<timestamp>, [AUTH-1041], <sequence-number>,, ERROR, <system-name>, Port <port number> has been disabled, because an authentication-reject was received with code '<Reason String>' and explanation '<Explanation String>'.`

Probable cause The specified port had been disabled, because it received an authentication-reject response from the connected switch/device. The error might indicate that an invalid entity attempted to connect to the switch.

Recommended action Check the connection port for a possible security attack.

Check the shared secrets using **secAuthSecret** and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

AUTH-1042

Message

```
<timestamp>, [AUTH-1042], <sequence-number>,, ERROR,
<system-name>, Port <port number> has been disabled,
because authentication failed with code '<Reason String>'
and explanation '<Explanation String>'.
```

Probable cause

The specified port has been disabled, because the connecting switch/device failed to authenticate. The error might indicate that an invalid entity attempted to connect to the switch.

Recommended action

Check the connection port for a possible security attack.

Check the shared secrets using **secAuthSecret** and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

AUTH-1043

Message

```
<timestamp>, [AUTH-1043], <sequence-number>,, ERROR,
<system-name>, Failed to enforce device authentication
mode:<Device Auth Policy>(error: <Reason Code>).
```

Probable cause

Indicates that the Kernel mode setting for F_Port authentication failed. Device authentication will be defaulted to OFF, and the switch will not participate in Diffie Hellman - challenge handshake authentication protocol (DH-CHAP) authentication with devices.

Recommended action

Try setting the device authentication policy manually using the **authUtil** command.

Severity

ERROR

AUTH-1044

Message

```
<timestamp>, [AUTH-1044], <sequence-number>,, ERROR,
<system-name>, Authentication <Reason for disabling the
port>. Disabling port <port number>.
```

Probable cause Indicates authentication has timed out after multiple retries. The specified port has been disabled as a result. This problem may be transient due to the system's central processing unit (CPU) load. In addition, a defective small form-factor pluggable (SFP) or faulty cable may have caused the failure.

Recommended action Check the SFP and the cable. Then try to enable the port using the **portEnable** command.

Severity ERROR

4

BKSW System Messages

This chapter contains information on the following BKSW message:

- BKSW-1003 116

BKSW-1003

Message

```
<timestamp>, [BKSW-1003], <sequence-number>,, WARNING,
<system-name>, kSWD: <warning message>.
```

Probable cause

Indicates a warning state within the system.

A critical application error was reported in the watchdog subsystem. This message is used to convey information regarding the state of the system. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or failover (on dual-CP switches).

The *warning message* might be any one of the following:

- <Detected unexpected termination of: <daemon name>>
  Probable cause: One of the critical daemons ended unexpectedly.
- <<daemon name> failed to refresh SWD*** Sending SIGABRT to PID <process id number>>
  Probable cause: One of the critical daemons is found to be nonresponsive; sending signal abort.

Recommended action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

5

BL System Messages

This chapter contains information on the following BL messages:

- BL-1000 119
- BL-1001 119
- BL-1002 119
- BL-1003 120
- BL-1004 120
- BL-1006 121
- BL-1007 121
- BL-1008 122
- BL-1009 122
- BL-1010 123
- BL-1011 123
- BL-1012 124
- BL-1013 124
- BL-1014 125
- BL-1015 126
- BL-1016 126
- BL-1017 127
- BL-1018 127
- BL-1019 127
- BL-1020 128
- BL-1021 128
- BL-1022 129
- BL-1023 129
- BL-1024 130
- BL-1025 130
- BL-1026 130
- BL-1027 131

- BL-1028 131
- BL-1029 131
- BL-1030 132
- BL-1031 132
- BL-1032 133
- BL-1033 133
- BL-1034 134
- BL-1035 134
- BL-1036 134
- BL-1037 135

BL-1000

Message

```
<timestamp>, [BL-1000], <sequence-number>,, INFO,
<system-name>, Initializing ports...
```

Probable cause

Indicates that the switch has started initializing the ports.

Recommended action

No action is required.

Severity

INFO

BL-1001

Message

```
<timestamp>, [BL-1001], <sequence-number>,, INFO,
<system-name>, Port initialization completed.
```

Probable cause

Indicates that the switch has completed initializing the ports.

Recommended action

No action is required.

Severity

INFO

BL-1002

Message

```
<timestamp>, [BL-1002], <sequence-number>, FFDC,
CRITICAL, <system-name>, Init Failed: slot <slot number>
DISABLED because internal ports were not ONLINE, <list of
internal port number not ONLINE>.
```

Probable cause

Indicates that the blade initiation failed because one or more of the internal ports were not online. The blade is faulted.

Recommended action

Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Note that any reference seen to slot 0 is a reference to the blade within the switch platform, e.g., MP-7500B and AP-7600B contain PB-48K-18i and PB-48K-AP4-18 blades respectively.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

Additional blade fault messages precede and follow this error, providing more information. See other error messages for recommended action.

If the message persists, replace the blade.

Severity CRITICAL

BL-1003

Message

```
<timestamp>, [BL-1003], <sequence-number>, FFDC,
CRITICAL, <system-name>, Faulting blade in slot <slot
number>.
```

Probable cause Indicates a faulty blade in the specified slot number.

Recommended action Make sure that the blade is seated correctly. If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1004

Message

```
<timestamp>, [BL-1004], <sequence-number>, FFDC,
CRITICAL, <system-name>, Suppressing blade fault in slot
<slot number>.
```

Probable cause Indicates that the specified blade experienced a failure but was not faulted due to a user setting.

Recommended action Reboot or power cycle the blade, using the **slotPowerOff** and **slotPowerOn** commands.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1006

Message

```
<timestamp>, [BL-1006], <sequence-number>,, INFO,
<system-name>, Blade <slot number> NOT faulted. Peer
blade <slot number> experienced abrupt failure.
```

Probable cause Indicates that the errors (mostly synchronization errors) on this blade are harmless. Probably, the standby control processor (CP) blade connected to the active CP blade has experienced transitory problems.

Recommended action Use the **haShow** command to verify that the standby CP is healthy. If the standby CP was removed or faulted by user intervention, no action is required.

Severity INFO

BL-1007

Message

```
<timestamp>, [BL-1007], <sequence-number>,, WARNING,
<system-name>, blade #<blade number>: blade state is
inconsistent with EM. bl_cflags 0x<blade control flags>,
slot_on <slot_on flag>, slot_off <slot_off flag>, faulty
<faulty flag>, status <blade status>.
```

Probable cause Indicates that a failover occurred while a blade was initializing on the previously active control processor (CP).

Recommended action No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity WARNING

BL-1008

Message

```
<timestamp>, [BL-1008], <sequence-number>, FFDC,
CRITICAL, <system-name>, Slot <slot number> control-plane
failure. Expected value: 0x<value 1>, Actual: 0x<value
2>.
```

Probable cause

Indicates that the blade has experienced a hardware failure or was removed without following the recommended removal procedure.

Recommended action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1009

Message

```
<timestamp>, [BL-1009], <sequence-number>, FFDC,
CRITICAL, <system-name>, Blade in slot <slot number>
timed out initializing the chips.
```

Probable cause

Indicates that the blade has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1010

Message

```
<timestamp>, [BL-1010], <sequence-number>,, WARNING,
<system-name>, Blade in slot <slot number> inconsistent
with the hardware settings.
```

Probable cause

Indicates that a failover occurred while some hardware changes were being made on the previously active control processor (CP) (such as changing the domain ID).

Recommended action

No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity

WARNING

BL-1011

Message

```
<timestamp>, [BL-1011], <sequence-number>, FFDC,
CRITICAL, <system-name>, Busy with emb-port int. for chip
<chip number> in minis <minis number> on blade <slot
number>, chip int. is disabled. interrupt
status=0x<interrupt status>.
```

Probable cause

Indicates that too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the control processor (CP) from becoming too busy.

Recommended action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP), or device attached to the specified port.

Run the **systemVerification** command to verify that the blade or switch does not have hardware problems.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the nonbladed switch.

Severity CRITICAL

BL-1012

Message

```
<timestamp>, [BL-1012], <sequence-number>,, ERROR,
<system-name>, bport <port number> port int. is disabled.
status=0x<interrupt status> Port <port number> will be
re-enabled in 1 minute.
```

Probable cause Indicates that the port generated an excessive number of interrupts that might prove unrecoverable to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP), or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the nonbladed switch.

Severity ERROR

BL-1013

Message

```
<timestamp>, [BL-1013], <sequence-number>,, ERROR,
<system-name>, bport <port number> port is faulted.
status=0x<interrupt status> Port <port number> will be
re-enabled in 1 minute.
```

Probable cause Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP), or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, reboot or power cycle the switch.

If the message persists, replace the blade.

Severity

ERROR

BL-1014

Message

```
<timestamp>, [BL-1014], <sequence-number>,, ERROR,
<system-name>, bport <port number> port int. is disabled.
status=0x<interrupt status>.
```

Probable cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended action

Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On a bladed system, replace the blade field-replaceable unit (FRU).
- On all others, replace the switch.

Severity

ERROR

BL-1015

Message

```
<timestamp>, [BL-1015], <sequence-number>,, ERROR,
<system-name>, bport <port number> port is faulted.
status=0x<interrupt status>.
```

Probable cause

Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended action

Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On a bladed system, replace the blade field-replaceable unit (FRU).
- On all others, replace the switch.

Severity

ERROR

BL-1016

Message

```
<timestamp>, [BL-1016], <sequence-number>, FFDC,
CRITICAL, <system-name>, Blade port <port number> in slot
<slot number> failed to enable.
```

Probable cause

Indicates that the specified blade port has failed to get enabled.

Recommended action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1017

Message

```
<timestamp>, [BL-1017], <sequence-number>,, INFO,
<system-name>, Slot <slot number> Initializing...
```

Probable cause Indicates that the slot has started initializing the ports.

Recommended action No action is required.

Severity INFO

BL-1018

Message

```
<timestamp>, [BL-1018], <sequence-number>,, INFO,
<system-name>, Slot <slot number> Initialization
completed.
```

Probable cause Indicates that the slot has completed initializing the ports.

Recommended action No action is required.

Severity INFO

BL-1019

Message

```
<timestamp>, [BL-1019], <sequence-number>,, INFO,
<system-name>, Slot <Slot number>, retry <Retry Number>,
internal port retry initialization, <List of internal
ports retrying initialization>.
```

Probable cause Indicates that the slot had internal ports not online and that the system is retrying to bring the ports that failed back online.

Recommended action No action is required.

Severity INFO

BL-1020

Message

```
<timestamp>, [BL-1020], <sequence-number>,, CRITICAL,
<system-name>, Switch timed out initializing the chips.
```

Probable cause Indicates that the switch has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended action Reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

If the message persists, replace the switch.

Severity CRITICAL

BL-1021

Message

```
<timestamp>, [BL-1021], <sequence-number>,, INFO,
<system-name>, Retry <Retry Number>, internal port retry
initialization, <List of internal ports retrying
initialization>.
```

Probable cause Indicates that the switch had internal ports not online and that the system is retrying to bring the ports that failed back online.

Recommended action No action is required.

Severity INFO

BL-1022

Message

```
<timestamp>, [BL-1022], <sequence-number>,, CRITICAL,
<system-name>, Init Failed: Switch DISABLED because
internal ports were not ONLINE, <list of internal port
number not ONLINE>.
```

Probable cause

Indicates that the switch initiation failed because one or more of the internal ports was not online. The switch is faulted.

Recommended action

Reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on these commands.

Additional fault messages precede and follow this error, providing more information. See other error messages for recommended action.

If the message persists, replace the switch.

Severity

CRITICAL

BL-1023

Message

```
<timestamp>, [BL-1023], <sequence-number>,, CRITICAL,
<system-name>, Blade in slot <slot number> was reset
before blade init completed. As a result the blade is
faulted.
```

Probable cause

Indicates that the blade was reset before the initialization completed.

Recommended action

Reboot or power cycle the blade.

If the message persists, replace the blade.

Severity

CRITICAL

BL-1024

Message

```
<timestamp>, [BL-1024], <sequence-number>,, INFO,
<system-name>, All ports on the blade in slot <slot
number> will be reset as part of the firmware upgrade.
```

Probable cause Indicates that a recent firmware upgrade caused the blade's firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all datapath elements were reset.

Recommended action No action is required.

Severity INFO

BL-1025

Message

```
<timestamp>, [BL-1025], <sequence-number>,, INFO,
<system-name>, All GigE/FCIP Virtualization ports on the
blade in slot <slot number> will be reset as part of the
firmware upgrade.
```

Probable cause Indicates that a recent firmware upgrade caused the blade's firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all GigE/Fibre Channel over IP (FCIP) Virtualization data elements were reset.

Recommended action No action is required.

Severity INFO

BL-1026

Message

```
<timestamp>, [BL-1026], <sequence-number>,, CRITICAL,
<system-name>, Internal port offline during warm
recovery, state <port state> (0x<port ID>).
```

Probable cause Indicates that an internal port went offline during the warm recovery of the switch. The switch will reboot and start a cold recovery.

Recommended action Collect **supportSave** information, then reboot switch and run the **diagPost** command to ensure Power-On Self-Test (POST) is enabled. If problem persists, replace the switch.

Severity CRITICAL

BL-1027

Message

```
<timestamp>, [BL-1027], <sequence-number>,, CRITICAL,
<system-name>, Blade in slot <slot number> faulted, boot
failed; status 0x<boot status> 0x<1250 0 boot status>
0x<1250 1 boot status>.
```

Probable cause Indicates that the blade failed to boot properly.

Recommended action Reboot or power cycle the blade.

If the message persists, replace the blade.

Severity CRITICAL

BL-1028

Message

```
<timestamp>, [BL-1028], <sequence-number>,, CRITICAL,
<system-name>, Switch faulted; internal processor was
reset before switch init completed.
```

Probable cause Indicates that the switch's internal processor was reset before the initialization completed.

Recommended action Reboot or power cycle the switch.

If the message persists, replace the switch.

Severity CRITICAL

BL-1029

Message

```
<timestamp>, [BL-1029], <sequence-number>,, INFO,
<system-name>, All ports on the switch will be reset as
part of the firmware upgrade.
```

Probable cause Indicates that a recent firmware upgrade caused the switch's internal processor firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all the datapath elements were reset.

Recommended action No action is required.

Severity INFO

BL-1030

Message

```
<timestamp>, [BL-1030], <sequence-number>,, INFO,
<system-name>, All GigE/FCIP Virtualization/FC Fastwrite
ports on the switch will be reset as part of the firmware
upgrade.
```

Probable cause Indicates that a recent firmware upgrade caused the switch's internal processor firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all the GigE/Fibre Channel over IP (FCIP)/Virtualization data elements / FC Fastwrite ports were reset.

Recommended action No action is required.

Severity INFO

BL-1031

Message

```
<timestamp>, [BL-1031], <sequence-number>,, CRITICAL,
<system-name>, Link timeout in internal port (slot <Slot
number>, port <Port number>) resulted in blade fault. Use
slotpoweroff/slotpoweron to recover the blade.
```

Probable cause Indicates that link timeout occurred in one of the backend internal ports.

Recommended action Power cycle the blade or run the **slotPowerOff** and **slotPowerOn** commands.

Severity CRITICAL

BL-1032

Message

```
<timestamp>, [BL-1032], <sequence-number>,, CRITICAL,
<system-name>, (slot <slot number>,bitmap 0x<object
control flags(bitmap)>) ports never came up ONLINE
(reason <reason for port disable>, state <status of the
blade>). Disabling slot.
```

Probable cause

Indicates that back-end (non-user) ports have not come ONLINE within time limit.

Recommended action

Reboot or power cycle the blade. Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. If the message persists, replace the blade.

Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on the **systemVerification** command.

Severity

CRITICAL

BL-1033

Message

```
<timestamp>, [BL-1033], <sequence-number>,, CRITICAL,
<system-name>, (slot <slot number>,bitmap 0x<object
control flags(bitmap)>) No disable acknowledgment from
ports (state <status of the blade>). Disabling slot.
```

Probable cause

Indicates that the system timed out while waiting for disable messages from the user ports after disabling the ports.

Recommended action

Reboot or power cycle the blade. Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. If the message persists, replace the blade.

Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on the **systemVerification** command.

Severity

CRITICAL

BL-1034

Message `<timestamp>, [BL-1034], <sequence-number>,, INFO, <system-name>, Slot <slot number> FC Initialization completed.`

Probable cause Indicates that the indicated slot has completed initializing Fibre Channel (FC) ports.

Recommended action No action is required.

Severity INFO

BL-1035

Message `<timestamp>, [BL-1035], <sequence-number>,, INFO, <system-name>, Slot <slot number> iSCSI port <iscsi port number> Initialization completed.`

Probable cause Indicates that the indicated slot has completed initializing the specified iSCSI port.

Recommended action No action is required.

Severity INFO

BL-1036

Message `<timestamp>, [BL-1036], <sequence-number>,, CRITICAL, <system-name>, Faulting 8G blade in slot = <slot number> due to incompatible stag mode. All EX/VEX ports must be disabled in order to enable the 8G blade in the chassis.`

Probable cause In FOS 6.0, an 8G blade with legacy mode (EX_Port having stag) will be disabled.

Recommended action Disable all EX/VEX_Ports and perform a **slotpoweroff / slotPowerOn** on the 8G blade. All EX/VEX_ Ports can now be reenabled.

Severity CRITICAL

BL-1037

Message

```
<timestamp>, [BL-1037], <sequence-number>,, CRITICAL,
<system-name>, Faulting chip in slot = <slot number>,
miniS = <miniS number>,port = <port number> due to BE/BI
port fault.
```

Probable Cause

A possible hardware issue faulted the chip and disabled all the ports on that chip.

Recommended Action

Reboot or power cycle the blade. Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

If the problem persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

6

BLL System Messages

This chapter contains information on the following BLL message:

- BLL-1000 138

BLL-1000

Message

```
<timestamp>, [BLL-1000], <sequence-number>, FFDC,
CRITICAL, <system-name>, ASIC driver detected Slot <slot
number> port <port number> as faulty (reason: <reason>)
```

Probable cause

Indicates that a blade regulation problem was reported on the specified *slot number*. The blade is faulted.

The possible reason codes are as follows:

- 1 = Available buffer overflow
- 2 = Backend port buffer timeout
- 3 = Backend port got shut down
- 4 = Embedded port buffer timeout
- 5 = Excessive busy mini buffer
- 6 = Excessive RCC VC on E_Port
- 7 = Excessive RCC VC on FL_Port
- 8 = Fail detection buffer tag error
- 9 = Fail detection TX parity error
- 10 = EPI CMEM interrupt error
- 11 = CMI interrupt error
- 12 = Interrupt overrun
- 13 = FDET interrupt
- 14 = Interrupt suspended
- 15 = Filter LISTD error
- 16 = Unknown filter LIST error
- 17 = Wait for LPC open state
- 18 = Wait for Old port state
- 19 = Wait for Open init state
- 20 = TX parity error
- 21 = RAM parity error
- 22 = BISR or RAMINIT error

Recommended action

Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Guide* for more information on this command.

If the message persists, replace the blade.

Severity

CRITICAL

7

BM System Messages

This chapter contains information on the following BM messages:

- BM-1001 142
- BM-1002 142
- BM-1003 143
- BM-1004 143
- BM-1005 143
- BM-1006 144
- BM-1007 144
- BM-1008 145
- BM-1009 145
- BM-1054 146
- BM-1055 146
- BM-1056 147
- BM-1058 147

BM-1001

Message

```
<timestamp>, [BM-1001], <sequence-number>,, ERROR,
<system-name>, BM protocol version <Protocol version> in
slot <Slot number>.
```

Probable cause

Indicates that the software running on the CP cannot communicate with the AP blade in the indicated slot, in order to determine AP blade's firmware version. This can be due to one of the following:

- The CP blade is running a later version than the AP blade.
- The CP blade is running a much older version than the AP blade.

Recommended action

The problem can be corrected by changing the firmware version on either the control processor (CP) or on the application processor (AP) blade. The firmware version on the CP blade can be changed using the **firmwareDownload** command. Refer to the release notes to determine whether a non-disruptive firmware download is supported between the versions. As the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If needed, replace the AP blade.

Severity

ERROR

BM-1002

Message

```
<timestamp>, [BM-1002], <sequence-number>,, INFO,
<system-name>, Connection established between CP and
blade in slot <Slot number>.
```

Probable cause

The control processor (CP) has established a connection to the blade processor (BP) and can communicate.

Recommended action

No action is required.

Severity

INFO

BM-1003

Message

```
<timestamp>, [BM-1003], <sequence-number>,, WARNING,
<system-name>, Failed to establish connection between CP
and blade in slot <Slot number>. Faulting blade.
```

Probable cause

The control processor (CP) could not establish a connection to the blade processor (BP) to communicate.

Recommended action

Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

Severity

WARNING

BM-1004

Message

```
<timestamp>, [BM-1004], <sequence-number>,, INFO,
<system-name>, Blade firmware <Blade firmware> on slot <
Slot > is not consistent with system firmware <System
firmware>. Auto-leveling blade firmware to match system
firmware.
```

Probable cause

The policy of the specified blade is to auto-level the blade firmware to the system firmware. The inconsistency may be due to either of the following reasons:

- Blade firmware was detected to be different from the control processor (CP) firmware due to a firmware upgrade.
- The blade was just inserted and had a different version of the firmware loaded.

Recommended action

No action is required. The blade will automatically download the updated firmware.

Severity

INFO

BM-1005

Message

```
<timestamp>, [BM-1005], <sequence-number>,, WARNING,
<system-name>, Firmwaredownload timed-out for blade in
slot <Slot>. Faulting blade.
```

Probable cause The **firmwareDownload** command failed for the blade in the specified slot.

Recommended action Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade. On the MP-7500B or AP-7600B, switch off and on all primary power in order to power-cycle the unit.

Severity WARNING

BM-1006

Message

```
<timestamp>, [BM-1006], <sequence-number>,, INFO,
<system-name>, Blade is not configured. Persistently
disabling all ports for blade in slot <Slot number>.
```

Probable cause The policy of the specified blade is set to persistently disable all ports the first time the blade is detected. The message indicates either of the following:

- The blade was detected in this slot for the first time.
- The blade was configured under a different mode.

Recommended action Configure the blade so that it will persistently enable the ports.

Severity INFO

BM-1007

Message

```
<timestamp>, [BM-1007], <sequence-number>,, INFO,
<system-name>, Clearing EX/VEX/FC port configuration for
all ports for blade in slot <Slot number>.
```

Probable cause The specified blade was detected for the first time after a PB-48K-18i was previously configured in the same slot. The new blade requires the specified port configurations to be cleared.

Recommended action The blade ports are cleared automatically. No action is required.

Severity INFO

BM-1008

Message

```
<timestamp>, [BM-1008], <sequence-number>,, WARNING,
<system-name>, Download of blade firmware failed for
blade in slot <slot>. Reissue firmwaredownload to
recover.
```

Probable cause

The automatic firmware upgrade on the blade has failed because the blade firmware version was detected to be different from the control processor (CP) firmware version.

Recommended action

Issue the **firmwareDownload** command to recover the blade.

Severity

WARNING

BM-1009

Message

```
<timestamp>, [BM-1009], <sequence-number>,, WARNING,
<system-name>, Firmwaredownload timed-out for application
processor. Faulting switch.
```

Probable cause

The **firmwareDownload** on the application processor (AP) blade failed.

Recommended action

Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade. On the MP-7500B or AP-7600B, switch off and on all primary power in order to power-cycle the unit.

Severity

WARNING

BM-1010

Message

```
<timestamp>, [BM-1010], <sequence-number>,, INFO,
<system-name>, Resetting port configuration and linkcost
for all ports for blade in slot <slot number>.
```

Probable cause

The specified blade was detected for the first time after a PB-48K-10G-6 was previously configured in the same slot. The new blade requires resetting the port configuration and linkcost.

Recommended action

The blade ports are cleared automatically. No action is required.

Severity INFO

BM-1053

Message `<timestamp>, [BM-1053], <sequence-number>,, WARNING, <system-name>, Failed to establish connection between CP and Application Processor. Faulting switch.`

Probable cause The control processor (CP) could not establish a connection to the application processor to communicate.

Recommended action On the MP-7500B or AP-7600B, switch off and on all primary power to power-cycle the unit.

Severity WARNING

BM-1054

Message `<timestamp>, [BM-1054], <sequence-number>,, INFO, <system-name>, AP firmware <Blade firmware> is not consistent with system firmware <System firmware>. Auto-leveling AP firmware to match system firmware.`

Probable cause The policy of the specified blade is set to auto-level the blade firmware to the system firmware, so either:

- Blade firmware was detected to be different from CP firmware due to a firmware upgrade.
- The blade was just inserted and had a different firmware loaded.

Recommended action No action is required. The blade will automatically download the updated firmware.

Severity INFO

BM-1055

Message `<timestamp>, [BM-1055], <sequence-number>,, WARNING, <system-name>, Firmwaredownload timed-out for AP. Faulting switch.`

Probable cause The **firmwareDownload** command on the application processor (AP) blade failed.

Recommended action Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade. On the MP-7500B or AP-7600B, switch off and on all primary power in order to power-cycle the unit.

Severity WARNING

BM-1056

Message

```
<timestamp>, [BM-1056], <sequence-number>,, INFO,
<system-name>, AP is not configured. Persistently
disabling all ports on the switch.
```

Probable cause The policy of the specified switch is to persistently disable all ports the first time the application processor (AP) blade is detected. This may be caused by one of the following:

- The AP was detected for the first time on this switch.
- The switch was configured under a different mode.

Recommended action Configure the switch to persistently enable all ports.

Severity INFO

BM-1058

Message

```
<timestamp>, [BM-1058], <sequence-number>,, WARNING,
<system-name>, Download of AP firmware failed for the
switch. Reissue firmwaredownload to recover.
```

Probable cause The automatic firmware upgrade on the application processor (AP) has failed because the firmware version running on the AP was detected to be different from system firmware due to a firmware upgrade.

Recommended action Issue the **firmwareDownload** command to recover the AP.

Severity WARNING

8

C2 System Messages

This chapter contains information on the following C2 system messages:

- C2-1001 150
- C2-1002 150
- C2-1004 150
- C2-1005 151

C2-1001

Message

```
<timestamp>, [C2-1001], <sequence-number>,, ERROR,
<system-name>, Port <port number> port fault (the
configured speed may not be supported by the SFP). Please
change the SFP or check the cable.
```

Probable Cause Indicates a deteriorated SFP, an incompatible SFP pair, or a faulty cable between the peer ports.

Recommended Action Verify that you are using compatible SFPs on the peer ports. Verify that the SFPs have not deteriorated and the Fibre Channel cable is not faulty. Replace SFPs or cable if necessary.

Severity ERROR

C2-1002

Message

```
<timestamp>, [C2-1002], <sequence-number>,, ERROR,
<system-name>, Port <port number> chip faulted due to an
internal error.
```

Probable Cause Internal error. All the ports on the blade/switch will be disrupted.

Recommended Action For a bladed system, perform a **slotPowerOff** and **slotPowerOn** on the blade to recover the system. For a non-bladed system, perform a **fastboot** on the switch to recover the system.

Severity ERROR

C2-1004

Message

```
<timestamp>, [C2-1004], <sequence-number>,, ERROR,
<system-name>, <slot number>,<chip index>: Invalid DMA ch
pointer, chan:<Channel number>, good_addr:<Good address>
bad_addr:<Bad address>
```

Probable Cause Indicates an internal error in the Application-Specific Integrated Circuit (ASIC) hardware that may degrade data traffic.

Recommended Action Whenever this error is observed, reboot the system at the next maintenance window. If the problem persists, replace the blade.

Severity ERROR

C2-1005

Message `<timestamp>, [C2-1005], <sequence-number>,, ERROR, <system-name>, Rate limit configuration is not effective on S(<slot number>) user port <port number> because QoS license is not present.`

Probable Cause Indicates that the switch does not have the QoS license added. Rate Limit is a licensed feature and requires a QoS license.

Recommended Action Add a QoS license to the switch to enable the Rate Limit functionality.

Severity ERROR

9 CDR System Messages

This chapter contains information on the following CDR messages:

- CDR-1001 154
- CDR-1002 154
- CDR-1003 154
- CDR-1004 155

CDR-1001

Message

```
<timestamp>, [CDR-1001], <sequence-number>,, ERROR,
<system-name>, Port <port number> port fault. Please
change the SFP or check cable
```

Probable cause

Indicates a deteriorated small form-factor pluggable (SFP), an incompatible SFP pair, a faulty cable between peer ports, or the port speed configuration does not match the capability of the SFP.

Recommended action

Verify that you are using compatible SFPs on the peer ports.

Verify that the SFPs have not deteriorated and that the Fibre Channel cable is not faulty. Replace the SFPs or cable if necessary. If there is a speed configuration mismatch, replace the SFP with a compatible one or change the configuration.

Severity

ERROR

CDR-1002

Message

```
<timestamp>, [CDR-1002], <sequence-number>, FFDC, ERROR,
<system-name>, Port <port number> chip faulted due to
internal error.
```

Probable cause

Internal error.

Recommended action

For a bladed system, issue the **slotPowerOff** and **slotPowerOn** commands on the blade to recover the system. For a non-bladed system, perform **fastBoot** on the switch to recover the system.

Severity

ERROR

CDR-1003

Message

```
<timestamp>, [CDR-1003], <sequence-number>, FFDC,
CRITICAL, <system-name>, <slot number>, <chip index> HW
ASIC chip error type =0<chip error>
```

Probable cause

Indicates an internal error in the application specific integrated circuit (ASIC) hardware that may degrade data traffic.

Recommended action Whenever this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the blade.

Severity CRITICAL

CDR-1004

Message `<timestamp>, [CDR-1004], <sequence-number>, FFDC, ERROR, <system-name>, <slot number>, <chip index>: invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address>, bad_addr:0x<Bad address>.`

Probable cause Indicates an internal error in the application specific integrated circuit (ASIC) hardware that may degrade data traffic.

Recommended action Whenever this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the blade.

Severity ERROR

10

CER System Messages

This chapter contains information on the following CER message:

- CER-1001 158

CER-1001

Message

```
<timestamp>, [CER-1001], <sequence-number>,, ERROR,
<system-name>, HA Sync broken, since standby Advanced
Performance Tuning module does not support FICON
Management Server (FMS).
```

Probable cause

Indicates that the high-availability (HA) synchronization between the active and standby control processors (CPs) is broken, because there is downlevel firmware loaded on the standby CP. The standby CP does not support the Advanced Performance Tuning module when the fibre connectivity (FICON) Management Server is enabled.

Recommended action

Run the **firmwareDownload** command to upgrade the firmware on the standby CP.

You can also disable FMS on the active CP.

Severity

ERROR

11

CHASSIS System Messages

This chapter contains information on the following CHASSIS messages:

- CHASSIS-1002 160
- CHASSIS-1003 160
- CHASSIS-1004 160
- CHASSIS-1005 161

CHASSIS-1002

Message `<timestamp>, [CHASSIS-1002], <sequence-number>,, ERROR, <system-name>, ki_gd_register_action failed with rc =<ret val>.`

Probable Cause Indicates an internal error.

Recommended Action For a bladed system, run the **slotPowerOff** command and **slotPowerOn** command on the blade to recover the system. For a non-bladed system, run the **fastBoot** command on the switch to recover the system.

Severity ERROR

CHASSIS-1003

Message `<timestamp>, [CHASSIS-1003], <sequence-number>,, ERROR, <system-name>, Slot ENABLED but Not Ready during recovery, disabling slot = <slot number> rval = <return value>.`

Probable Cause Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action On a bladed system, run the **slotPowerOff** command followed by the **slotPowerOn** command. On a non-bladed switch, reboot or power cycle the switch.

Severity ERROR

CHASSIS-1004

Message `<timestamp>, [CHASSIS-1004], <sequence-number>,, ERROR, <system-name>, Blade attach failed during recovery, disabling slot = <slot number>, rval = <return value>.`

Probable Cause Indicates that a blade has failed during failover or recovery.

Recommended Action On a bladed system , run the **slotPowerOff** command followed by the **slotPowerOn** command. On a non-bladed switch, reboot or power cycle the switch.

Severity ERROR

CHASSIS-1005

Message `<timestamp>, [CHASSIS-1005], <sequence-number>,, ERROR, <system-name>, Diag attach failed during recovery, disabling slot = <slot number>.`

Probable Cause Indicates that the Diag blade attach has failed during failover or recovery.

Recommended Action On a bladed system, run the **slotPowerOff** command followed by the **slotPowerOn** command. On a non-bladed switch, reboot or power cycle the switch.

Severity ERROR

12 CONF System Messages

This chapter contains information on the following CONF messages:

- CONF-1000 164
- CONF-1001 164
- CONF-1020 164
- CONF-1021 165
- CONF-1022 165
- CONF-1030 165

CONF-1000

Message

```
<timestamp>, [CONF-1000], <sequence-number>, AUDIT, INFO,
<system-name>, configDownload completed successfully.
<Info about the parameters and AD>.
```

Probable cause

Indicates that the **configDownload** operation was initiated and completed successfully. The message string that follows is a description of the class of configuration parameters that were downloaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

Recommended action

No action is required.

Severity

INFO

CONF-1001

Message

```
<timestamp>, [CONF-1001], <sequence-number>,, INFO,
<system-name>, configUpload completed successfully. <Info
about the parameters and AD>.
```

Probable cause

Indicates that the **configUpload** operation was initiated and completed successfully. The message string that follows is the description of the class of configuration parameters that were uploaded. If AD is enabled, the AD number is specified in the description.

Recommended action

No action is required.

Severity

INFO

CONF-1020

Message

```
<timestamp>, [CONF-1020], <sequence-number>,, INFO,
<system-name>, configDownload not permitted <AD Number if
AD is configured on the system>.
```

Probable cause

Indicates a **configDownload** operation is not permitted. There are many possible causes.

Recommended action Check the error log for a possible cause. Correct the error and rerun **configDownload**.

Severity INFO

CONF-1021

Message

```
<timestamp>, [CONF-1021], <sequence-number>,, INFO,
<system-name>, configUpload not permitted <AD Number if
AD is configured on the system>.
```

Probable cause Indicates a **configUpload** operation is not permitted. There are many possible causes.

Recommended action Check the error log for a possible cause. Correct the error and rerun **configUpload.**

.Severity INFO

CONF-1022

Message

```
<timestamp>, [CONF-1022], <sequence-number>,, INFO,
<system-name>, Downloading configuration without
disabling the switch was unsuccessful.
```

Probable cause Indicates that an attempt to download the configuration without disabling the switch was unsuccessful because there are one or more parameters that require the switch to be disabled.

Recommended action Disable the switch and try to download configuration again.

Severity INFO

CONF-1030

Message

```
<timestamp>, [CONF-1030], <sequence-number>,, WARNING,
<system-name>, Configuration database full, data not
committed (key:<Key of failed configuration data>.
```

Probable cause Indicates that the previous configuration commands have resulted in a database full condition. Configuration changes associated with specified key have not been applied.

Recommended action Use configure and other various commands to erase unneeded configuration parameters. As a last resort, execute **configDefault** and re-configure the system.

Severity INFO

13 CTAP System Messages

This chapter contains information on the following CTAP message:

- CTAP-1001 168

CTAP-1001

Message

```
<timestamp>, [CTAP-1001], <sequence-number>,, INFO,
<system-name>, Key acquisition for <Pool or Container>
<Begins or Complete>.
```

Probable cause

Indicates that a change in the tape pool database has triggered the key acquisition process for each pool.

Recommended action

Do not start tape backup or restore operations involving tape pools until the process is complete.

Severity

INFO

14

CVLC System Messages

This chapter contains information on the following CVLC messages:

- CVLC-1001 170
- CVLC-1002 170
- CVLC-1003 170
- CVLC-1004 171
- CVLC-1005 171
- CVLC-1006 171
- CVLC-1008 172
- CVLC-1009 172
- CVLC-1010 172
- CVLC-1011 173
- CVLC-1012 173
- CVLC-1013 174
- CVLC-1014 174
- CVLC-1015 174
- CVLC-1016 175
- CVLC-1017 175
- CVLC-1018 175
- CVLC-1019 176
- CVLC-1020 176
- CVLC-1021 176
- CVLC-1021 176
- CVLC-1022 177

CVLC-1001

Message

```
<timestamp>, [CVLC-1001], <sequence-number>,, INFO,
<system-name>, <Re-key type (First time encryption/Key
expired/Manual)> re-key <Re-key action
(started/completed/failed/cancelled)>, LUN SN: <LUN
serial number>.\nContainer: <Target container name>,
Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates the *action* has been applied to a **First time encryption, Key expired** or **Manual re-key** operation. The *action* is one of started, completed, or cancelled.

Recommended Action No action is required.

Severity INFO

CVLC-1002

Message

```
<timestamp>, [CVLC-1002], <sequence-number>,, INFO,
<system-name>, Tape session <Tape session action
(started/cancelled/failed)>.\nContainer: <Target
container name>, Initiator: <Initiator physical WWN>, LUN
ID: <LUN ID>.
```

Probable Cause Indicates that a tape session has been started, cancelled, or failed.

Recommended Action No action is required.

Severity INFO

CVLC-1003

Message

```
<timestamp>, [CVLC-1003], <sequence-number>,, INFO,
<system-name>, Forceful LUN policy change to clear text
while re-key session is still active.\nContainer: <Target
container name>, Initiator: <Initiator physical WWN>, LUN
ID: <LUN ID>.
```

Probable Cause Indicates that the encryption LUN policy was forcefully changed while a re-key session was still active.

Recommended Action No action is required.

Severity INFO

CVLC-1004

Message

```
<timestamp>, [CVLC-1004], <sequence-number>,, INFO,
<system-name>, Forceful encryption LUN removal while
re-key session is still active.\nContainer: <Target
container name>, Initiator: <Initiator physical WWN>, LUN
ID: <LUN ID>.
```

Probable Cause Indicates that the encryption LUN was forcefully removed while a re-key session was still active.

Recommended Action No action is required.

Severity INFO

CVLC-1005

Message

```
<timestamp>, [CVLC-1005], <sequence-number>,, INFO,
<system-name>, There is no LUN's found from the
target.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that there are no LUNs found from the target-initiator pair.

Recommended Action No action is required.

Severity INFO

CVLC-1006

Message

```
<timestamp>, [CVLC-1006], <sequence-number>,, INFO,
<system-name>, Duplicate LUN serial number <LUN SN>
found.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>.
```

Probable Cause Indicates that there is more than one LUN serial number discovered from the same target. Therefore, encryption on this target is disabled.

Recommended Action No action is required.

Severity INFO

CVLC-1008

Message

```
<timestamp>, [CVLC-1008], <sequence-number>,, ERROR,
<system-name>, LUN discovery failure: <Discovery state>,
Container: <Target container name>, Initiator: <Initiator
physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that LUN discovery failed.

Recommended Action No action is required.

Severity ERROR

CVLC-1009

Message

```
<timestamp>, [CVLC-1009], <sequence-number>,, ERROR,
<system-name>, Wrong device type: should be <Expected
device type (Disk/Tape)>, found <Discovered device type
(Disk/Tape)>.\nContainer: <Target container name>,
Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the wrong device type was found.

Recommended Action No action is required.

Severity ERROR

CVLC-1010

Message

```
<timestamp>, [CVLC-1010], <sequence-number>,, ERROR,
<system-name>, Tape license is required for tape
container: <Target container name>.
```

Probable Cause Indicates that the tape container is configured for DataFort compatibility mode, but there is no valid license for it on the switch.

Recommended Action Install the DataFort compatibility license, using the **licenseAdd** command. Refer to your EMC account representative to obtain the license if you do not have one.

Severity ERROR

CVLC-1011

Message

```
<timestamp>, [CVLC-1011], <sequence-number>,, ERROR,
<system-name>, Third party license is required for
encryption LUN in third party mode.\nContainer: <Target
container name>, Initiator: <Initiator physical WWN>, LUN
ID: <LUN ID>.
```

Probable Cause Indicates that the encryption LUN is configured for DataFort compatibility mode, but there is no valid license for it on the switch.

Recommended Action Install the DataFort compatibility license, using the **licenseAdd** command. Refer to your EMC account representative to obtain the license if you do not have one.

Severity ERROR

CVLC-1012

Message

```
<timestamp>, [CVLC-1012], <sequence-number>,, ERROR,
<system-name>, Disk metadata is in wrong format
(<Metadata format found (Brocade/Third
party)>).\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the metadata found on the disk LUN is in the wrong format.

Recommended Action Use the **cryptocfg** command to change the LUN's metadata mode.

Severity ERROR

CVLC-1013

Message

```
<timestamp>, [CVLC-1013], <sequence-number>,, ERROR,
<system-name>, Unable to retrieve key record from the key
archive.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the encryption engine is unable to retrieve the key record base on the key ID found in the metadata.

Recommended Action No action is required.

Severity ERROR

CVLC-1014

Message

```
<timestamp>, [CVLC-1014], <sequence-number>,, ERROR,
<system-name>, Missing Key ID from user
input.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the data state in the LUN configuration is in the Encrypted state without a key ID and there is no metadata found on the LUN.

Recommended Action Use the **cryptocfg** command to add the key ID, if available.

Severity ERROR

CVLC-1015

Message

```
<timestamp>, [CVLC-1015], <sequence-number>,, ERROR,
<system-name>, LUN is set to read only mode. Reason:
<Reason for LUN is set to read only mode>.\nContainer:
<Target container name>, Initiator: <Initiator physical
WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the LUN is set as read only because there is a conflict in the configuration.

Recommended Action No action is required.

Severity ERROR

CVLC-1016

Message

```
<timestamp>, [CVLC-1016], <sequence-number>,, INFO,
<system-name>, LUN is out of read only mode. Reason:
<Reason for LUN is out of read only mode>.\nContainer:
<Target container name>, Initiator: <Initiator physical
WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the LUN is set back to read/write.

Recommended Action No action is required.

Severity INFO

CVLC-1017

Message

```
<timestamp>, [CVLC-1017], <sequence-number>,, INFO,
<system-name>, Event: <Description of the
event>.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates warning or error event.

Recommended Action No action is required.

Severity INFO

CVLC-1018

Message

```
<timestamp>, [CVLC-1018], <sequence-number>,, INFO,
<system-name>, Event: <Description of the
event>.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates an informational event.

Recommended Action No action is required.

Severity INFO

CVLC-1019

Message

```
<timestamp>, [CVLC-1019], <sequence-number>,, ERROR,
<system-name>, Metadata exists while data state is clear
text.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the data state in the LUN configuration is in clear text state but metadata exists on the LUN.

Recommended Action Use the **cryptocfg** command to confirm the configuration.

Severity ERROR

CVLC-1020

Message

```
<timestamp>, [CVLC-1020], <sequence-number>,, ERROR,
<system-name>, Metadata exists while LUN is clear
text.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that metadata exists on the LUN that is clear text.

Recommended Action Use the **cryptocfg** command to confirm the configuration.

Severity ERROR

CVLC-1021

Message

```
<timestamp>, [CVLC-1021], <sequence-number>,, INFO,
<system-name>, User provided key ID <Key ID from
metadata> is ignored while metadata <Key ID provided by
the user> exists.\nContainer: <Target container name>,
Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the key ID provided is ignored because metadata exists on the LUN.

Recommended Action No action is required.

Severity INFO

CVLC-1022

Message

```
<timestamp>, [CVLC-1022], <sequence-number>,, INFO,
<system-name>, User provided key ID <Key ID from
metadata> is ignored while data state is clear
text.\nContainer: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Probable Cause Indicates that the key ID provided is ignored because the data state is clear text.

Recommended Action No action is required.

Severity INFO

15

CVLM System Messages

This chapter contains information on the following CVLM messages:

- CVLM-1001 180
- CVLM-1002 180
- CVLM-1003 180
- CVLM-1004 181
- CVLM-1005 181
- CVLM-1006 181
- CVLM-1007 182
- CVLM-1008 182
- CVLM-1009 182
- CVLM-1010 183
- CVLM-1011 183
- CVLM-1012 183

CVLM-1001

Message

```
<timestamp>, [CVLM-1001], <sequence-number>,, ERROR,
<system-name>, Failed to allocate memory: (<function
name>).
```

Probable Cause

Indicates that the specified function failed to allocate memory.

Recommended Action

- Check memory usage on the switch using the **memShow** command.
- Reboot or power cycle the switch.

Severity

ERROR

CVLM-1002

Message

```
<timestamp>, [CVLM-1002], <sequence-number>,, ERROR,
<system-name>, Failed to initialize <module> rc =
<error>.
```

Probable Cause

Indicates that an initialization of a module within the Cavium security processor failed.

Recommended Action

Download a new firmware version using the **firmwareDownload** command.

Severity

ERROR

CVLM-1003

Message

```
<timestamp>, [CVLM-1003], <sequence-number>,, INFO,
<system-name>, Crypto device configuration has been
committed by switch (<Switch WWN>).
```

Probable Cause

Indicates the **cryptocfg --commit** status.

Recommended Action

No action is required.

Severity

INFO

CVLM-1004

Message

```
<timestamp>, [CVLM-1004], <sequence-number>,, WARNING,
<system-name>, Crypto device configuration between local
switch (<local switch WWN>) and peer (<peer switch WWN>)
is out of sync. New encryption session is not allowed.
```

Probable Cause Indicates that encryption engine nodes in the cluster encryption group have different configurations.

Recommended Action Synchronize the configuration in the cluster group using the **cryptocfg --commit** command.

Severity WARNING

CVLM-1005

Message

```
<timestamp>, [CVLM-1005], <sequence-number>,, INFO,
<system-name>, Crypto service is <status> on the switch.
```

Probable Cause Indicates that the Crypto service is enabled or disabled on the switch.

Recommended Action No action is required.

Severity INFO

CVLM-1006

Message

```
<timestamp>, [CVLM-1006], <sequence-number>,, WARNING,
<system-name>, Crypto device <device WWN> in target
container <container name> is not in AD0.
```

Probable Cause Indicates that the crypto device in the crypto target container is not in AD0.

Recommended Action Use the **ad** command to move the crypto device into Admin Domain 0.

Severity WARNING

CVLM-1007

Message `<timestamp>, [CVLM-1007], <sequence-number>,, WARNING, <system-name>, Redirect zone update failure. Status is <status>.`

Probable Cause Indicates that the redirect zone update failed.

Recommended Action Issue the **cryptocfg --commit** command again.

Severity WARNING

CVLM-1008

Message `<timestamp>, [CVLM-1008], <sequence-number>,, WARNING, <system-name>, The member (<EE node WWN> <EE slot num>) of HAC (<HAC name>) is not in the fabric.`

Probable Cause Indicates that the member of an HA cluster is not in the fabric.

Recommended Action Check the ISL port connected to the fabric.

Severity WARNING

CVLM-1009

Message `<timestamp>, [CVLM-1009], <sequence-number>,, INFO, <system-name>, The member (<EE node WWN> <EE slot num>) of HAC (<HAC name>) is in the fabric.`

Probable Cause Indicates that the member of an HA cluster is in the fabric.

Recommended Action No action is required.

Severity INFO

CVLM-1010

Message

```
<timestamp>, [CVLM-1010], <sequence-number>,, WARNING,
<system-name>, The IP address of EE (<EE node WWN> <EE
slot num>) IO link is not configured.
```

Probable Cause Indicates that the encryption engine IO link IP address is not configured.

Recommended Action Configure the encryption engine IO link IP address.

Severity WARNING

CVLM-1011

Message

```
<timestamp>, [CVLM-1011], <sequence-number>,, INFO,
<system-name>, The HAC failover occurs at EE (<EE node
WWN> <EE slot num>).
```

Probable Cause Indicates that the HA cluster failover occurred at the Encryption Engine (EE).

Recommended Action No action is required.

Severity INFO

CVLM-1012

Message

```
<timestamp>, [CVLM-1011], <sequence-number>,, INFO,
<system-name>, The HAC failback occurs at EE (<EE node
WWN> <EE slot num>).
```

Probable Cause Indicates that the HA cluster failback occurred at the Encryption Engine (EE).

Recommended Action No action is required.

Severity INFO

16

EM System Messages

This chapter contains information on the following EM messages:

- EM-1001 187
- EM-1002 187
- EM-1003 187
- EM-1004 188
- EM-1005 188
- EM-1006 189
- EM-1007 189
- EM-1008 190
- EM-1009 190
- EM-1010 191
- EM-1011 191
- EM-1012 191
- EM-1013 192
- EM-1014 192
- EM-1015 193
- EM-1016 193
- EM-1017 193
- EM-1018 194
- EM-1019 194
- EM-1028 194
- EM-1029 195
- EM-1031 195
- EM-1033 196
- EM-1034 196
- EM-1035 197
- EM-1036 197
- EM-1037 198

- EM-1041 198
- EM-1042 199
- EM-1043 199
- EM-1044 199
- EM-1045 200
- EM-1046 200
- EM-1047 201
- EM-1048 201
- EM-1049 202
- EM-1050 202
- EM-1051 202
- EM-1055 203
- EM-1056 203
- EM-1057 203
- EM-1058 204
- EM-1059 204
- EM-1060 205
- EM-1061 205
- EM-1062 205
- EM-1063 206
- EM-1064 206
- EM-1065 207
- EM-1066 207
- EM-1067 207
- EM-1068 208
- EM-1069 208
- EM-1070 209
- EM-2003 209

EM-1001

Message

```
<timestamp>, [EM-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU ID> is over heating:
Shutting down.
```

Probable cause

Indicates that a field-replaceable unit (FRU) is shutting down due to overheating. This is typically due to a faulty fan but can also be caused by the switch environment.

Recommended action

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced.

Severity

CRITICAL

EM-1002

Message

```
<timestamp>, [EM-1002], <sequence-number>, FFDC, INFO,
<system-name>, System fan(s) status <fan FRU>.
```

Probable cause

Indicates that a nonbladed system has overheated and may shut down. All fan speeds are dumped to the console.

Recommended action

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at high enough speed, they should be replaced.

Severity

INFO

EM-1003

Message

```
<timestamp>, [EM-1003], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU ID> has unknown hardware
identifier: FRU faulted.
```

Probable cause Indicates that a field-replaceable unit (FRU) header could not be read or is not valid. The FRU is faulted.

Recommended action On bladed systems, try reseating the specified FRU.

Reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on this command.

On bladed systems, replace the specified FRU.

For all others, replace the switch.

Severity CRITICAL

EM-1004

Message

```
<timestamp>, [EM-1004], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU ID> failed to power on.
```

Probable cause Indicates that a field-replaceable unit (FRU) failed to power on and is not being used. The type of FRU is specified in the message.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port.

The DS-220B has four fans and one power supply, and the DS-300B has three fans and one power supply, but these parts cannot be replaced; the entire switch is a FRU.

Recommended action Try reseating the FRU. If the message persists, replace the FRU.

Severity CRITICAL

EM-1005

Message

```
<timestamp>, [EM-1005], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU Id> has faulted. Sensor(s)
above maximum limits.
```

Probable cause Indicates that a blade in the specified slot or the switch (for nonbladed switches) is being shut down for environmental reasons; its temperature or voltage is out of range.

Recommended action Check the environment and make sure the room temperature is within the operational range of the switch. Use the **fanShow** command to verify fans are operating properly. Make sure there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

Severity CRITICAL

EM-1006

Message

```
<timestamp>, [EM-1006], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU Id> has faulted. Sensor(s)
below minimum limits.
```

Probable cause Indicates that the sensors show the voltage is below minimum limits. The switch or specified blade is being shut down for environmental reasons; the voltage is too low.

Recommended action If this problem occurs on a blade, it usually indicates a hardware problem on the blade; replace the blade.

If this problem occurs on a switch, it usually indicates a hardware problem on the main board; replace the switch.

Severity CRITICAL

EM-1007

Message

```
<timestamp>, [EM-1007], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU Id> is being reset.
Sensor(s) has exceeded max limits.
```

Probable cause Indicates that the voltage on a switch has exceeded environmental limits. A reset is sent to the faulty slot or the switch for nonbladed switches.

Recommended action

There is most likely a voltage hardware problem on the blade or motherboard of the switch.

On bladed systems, replace the specified FRU.

For all others, replace the switch.

Severity

CRITICAL

EM-1008

Message

```
<timestamp>, [EM-1008], <sequence-number>, FFDC,
CRITICAL, <system-name>, Unit in <Slot number or Switch>
with ID <FRU Id> is faulted, it is incompatible with the
<type of incompatibility> configuration.
```

Probable cause

Indicates that a blade inserted in the specified slot is not compatible with either the platform configuration or the logical switch configuration. The blade is faulted.

Recommended action

If the blade is not compatible, replace the blade and ensure the replacement blade is compatible with your control processor (CP) type. If the incompatibility is with the logical switch configuration, change the configuration with the **lscfg** command to be consistent with the blade type or remove the blade.

Severity

CRITICAL

EM-1009

Message

```
<timestamp>, [EM-1009], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU Id> powered down
unexpectedly.
```

Probable cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). This might indicate a hardware malfunction in the FRU.

Recommended action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

CRITICAL

EM-1010

Message

```
<timestamp>, [EM-1010], <sequence-number>, FFDC,
CRITICAL, <system-name>, Received unexpected power down
for <FRU Id> But <FRU Id> still has power.
```

Probable cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). However, the specified FRU still appears to be powered up after four seconds.

Recommended action

Try reseating the blade. If this fails to correct the error, replace the blade.

Severity

CRITICAL

EM-1011

Message

```
<timestamp>, [EM-1011], <sequence-number>, FFDC,
CRITICAL, <system-name>, Received unexpected power down
for <FRU Id>, but cannot determine if it has power.
```

Probable cause

Indicates that the environmental monitor (EM) received an unexpected power-down notification from the field-replaceable unit (FRU) specified; however, after four seconds it cannot be determined if it has powered down or not.

Recommended action

Try reseating the blade. If this fails to correct the error, replace the blade.

Severity

CRITICAL

EM-1012

Message

```
<timestamp>, [EM-1012], <sequence-number>, FFDC,
CRITICAL, <system-name>, <FRU Id> failed <state> state
transition, FRU faulted.
```

Probable cause

Indicates that a switch blade or nonbladed switch failed to transition from one state to another. It is faulted. The specific failed target state is displayed in the message. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended action

On bladed systems, try reseating the indicated field-replaceable unit (FRU).

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems.

If the message persists, replace the FRU.

Severity

CRITICAL

EM-1013

Message

```
<timestamp>, [EM-1013], <sequence-number>,, ERROR,
<system-name>, Failed to update FRU information for <FRU
Id>.
```

Probable cause

Indicates that the environmental monitor was unable to update the time alive or the original equipment manufacturer (OEM) data in the memory on a field-replaceable unit (FRU).

Recommended action

If you ran the **fruInfoSet** command, try the command again; otherwise, the update is automatically attempted again. If it continues to fail, try reseating the FRU.

If the message persists, replace the FRU.

Severity

ERROR

EM-1014

Message

```
<timestamp>, [EM-1014], <sequence-number>,, ERROR,
<system-name>, Unable to read sensor on <FRU Id> (<Return
code>)
```

Probable cause

Indicates that the environmental monitor was unable to access the sensors on the specified field-replaceable unit (FRU).

Recommended action

Try reseating the FRU. If the message persists, replace the FRU.

Severity

ERROR

EM-1015

Message

```
<timestamp>, [EM-1015], <sequence-number>,, WARNING,
<system-name>, Warm recovery failed (<Return code>).
```

Probable cause

Indicates that a problem was discovered when performing consistency checks during a warm boot.

Recommended action

Monitor the switch. If the problem persists, a **reBoot** or power cycle is required to resolve the problem.

Severity

WARNING

EM-1016

Message

```
<timestamp>, [EM-1016], <sequence-number>,, WARNING,
<system-name>, Cold recovery failed (<Return code>).
```

Probable cause

Indicates that a problem was discovered when performing consistency checks during a cold boot.

Recommended action

Monitor the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

EM-1017

Message

```
<timestamp>, [EM-1017], <sequence-number>,, WARNING,
<system-name>, Uncommitted WWN change detected. Cold
reboot required.
```

Probable cause

Indicates that a user did not commit a changed world-wide name (WWN) value prior to executing a **reboot**, power cycle, or **firmwareDownload** operation.

Recommended action

Change and commit the new WWN value.

Severity

WARNING

EM-1018

Message

```
<timestamp>, [EM-1018], <sequence-number>, FFDC,
CRITICAL, <system-name>, CP blade in slot <slot number>
failed to retrieve current chassis type (<detailed fault
descriptor>/<PLACE HOLDER>/0x<PLACE HOLDER>).
```

Probable cause Indicates that there was a failure to read the chassis type from the system.

Recommended action Verify that the control processor (CP) blade is operational and is properly seated in its slot.

Severity CRITICAL

EM-1019

Message

```
<timestamp>, [EM-1019], <sequence-number>,, WARNING,
<system-name>, Current chassis configuration option
(<Chassis config option currently in effect>) is not
compatible with standby firmware version (Pre 4.4),
cannot allow HA Sync.
```

Probable cause Indicates that the current **chassisConfig** option is not supported by the firmware on the standby control processor (CP). This is true even if the standby comes up and appears to be operational. High availability (HA) synchronization of the CPs will not be allowed.

Recommended action Either change the **chassisConfig** option to 1 with the **chassisConfig** command, or upgrade the firmware on the standby to the version running on the active CP.

Severity WARNING

EM-1028

Message

```
<timestamp>, [EM-1028], <sequence-number>, FFDC,
CRITICAL, <system-name>, HIL Error: <function> failed to
access history log for FRU: <FRU Id> (rc=<return code>).
```

Probable cause Indicates a problem accessing the data on the world-wide name (WWN) card field-replaceable unit (FRU), or the WWN card storage area on the main logic board.

The problems were encountered when the software attempted to write to the history log storage to record an event for the specified FRU. The return code is for internal use only. This is a serious hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port.

Recommended action If the message persists, reboot or power cycle the switch.

If the message still persists, replace the WWN card, or the switch (for nonbladed switches).

Severity CRITICAL

EM-1029

Message

```
<timestamp>, [EM-1029], <sequence-number>,, WARNING,
<system-name>, <FRU Id>, a problem occurred accessing a
device on the I2C bus (<error code>). Operational status
(<state of the FRU when the error occurred>) not changed,
access is being retried.
```

Probable cause Indicates that the I2C bus had problems and a timeout occurred.

Recommended action This is often a transient error.

Watch for the EM-1048 message, which indicates that the problem has been resolved.

If the error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the field-replaceable unit (FRU). If it continues to fail, replace the FRU.

Severity WARNING

EM-1031

Message

```
<timestamp>, [EM-1031], <sequence-number>,, ERROR,
<system-name>, <FRU Id> ejector not closed.
```

Probable cause Indicates that the environmental monitor (EM) has found a switch blade that is inserted, but the ejector switch is not closed. The blade in the specified slot is treated as not inserted.

Recommended action Close the ejector switch (raise the slider in most blades, or completely screw in the upper thumbscrew) if the field-replaceable unit (FRU) is intended for use. Refer to the appropriate hardware manual for instructions on inserting the switch blades.

Severity ERROR

EM-1033

Message

```
<timestamp>, [EM-1033], <sequence-number>,, ERROR,
<system-name>, CP in <FRU Id> set to faulty because CP
ERROR asserted
```

Probable cause Indicates that the standby control processor (CP) has been detected as faulty. The High Availability (HA) feature will not be available. This message occurs every time the other CP reboots, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the CP; however, you might want to find out why the failover occurred.

Recommended action If the standby CP was just rebooted, wait for the error to clear (run **slotShow** to determine if it has cleared). Watch for the EM-1047 message to verify that this error has cleared.

If the standby CP continues to be faulty or if it was not intentionally rebooted, check the error logs on the other CP (using the **errDump** command) to determine the cause of the error state.

Try reseating the field-replaceable unit (FRU). If the message persists, replace the FRU.

Severity ERROR

EM-1034

Message

```
<timestamp>, [EM-1034], <sequence-number>,, ERROR,
<system-name>, <FRU Id> set to faulty, rc=<return code>.
```

Probable cause Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended action Try reseating the FRU.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the FRU.

Severity ERROR

EM-1035

Message

```
<timestamp>, [EM-1035], <sequence-number>,, ERROR,
<system-name>, 2 circuit paired Power Supplies are
faulty, Check the <Switch side> AC main switch/circuit to
see if it has power.
```

Probable cause Suggests that since both Power Supplies associated with one of the two main circuits are present but faulty, maybe the circuit's switch has been turned off, or the AC power source has been interrupted for that circuit.

The *Switch side* value is either “left” or “right” designating which circuit switch, facing the cable side of the chassis. The *Switch side* value indicates:

- “left”: Controls the odd numbered power supply units.
- “right”: Controls the even numbered power supply units.

Recommended action Check that the identified AC circuit switch is turned on, that the power cord is properly attached and undamaged, and that the power source is operating properly.

Severity ERROR

EM-1036

Message

```
<timestamp>, [EM-1036], <sequence-number>,, WARNING,
<system-name>, <FRU Id> is not accessible.
```

Probable cause Indicates that the specified field-replaceable unit (FRU) does not seem to be present on the switch.

If the FRU is a world-wide name (WWN) card, then default WWN and IP addresses are used for the switch.

Recommended action

Reseat the FRU card.

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. Refer to the *EMC Connectrix B Series Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the FRU.

Severity

WARNING

EM-1037

Message

```
<timestamp>, [EM-1037], <sequence-number>,, INFO,
<system-name>, <FRU Id> is no longer faulted.
```

Probable cause

Indicates that the specified Power Supply has been marked as no longer being faulty, probably because its AC power supply has been turned on.

Recommended action

No action is required.

Severity

INFO

EM-1041

Message

```
<timestamp>, [EM-1041], <sequence-number>,, WARNING,
<system-name>, Sensor values for <FRU Id>: <Sensor Value>
<Sensor Value> <Sensor Value> <Sensor Value> <Sensor
Value> <Sensor Value> <Sensor Value>.
```

Probable cause

Indicates that sensors detected a warning condition. All significant sensors for the field-replaceable unit (FRU) are displayed; each contains a header.

This message can display:

- Voltages in volts
- Temperature in Celsius
- Fan speeds in RPM

Recommended action If the message is isolated, monitor the error messages on the switch. If the message is associated with other messages, follow the recommended action for those messages.

Severity WARNING

EM-1042

Message

```
<timestamp>, [EM-1042], <sequence-number>,, WARNING,
<system-name>, Important FRU header data for <FRU Id> is
not valid).
```

Probable cause Indicates that the specified field-replaceable unit (FRU) has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly or corrupted in the object database, which contains information about all FRUs.

Recommended action Try reseating the FRU. If the message persists, replace the FRU.

Severity WARNING

EM-1043

Message

```
<timestamp>, [EM-1043], <sequence-number>,, WARNING,
<system-name>, Can't power <FRU Id> <state (on or off)>.
```

Probable cause Indicates that the specified field-replaceable unit (FRU) cannot be powered on or off.

Recommended action The specified FRU is not responding to commands and should be replaced.

Severity WARNING

EM-1044

Message

```
<timestamp>, [EM-1044], <sequence-number>,, WARNING,
<system-name>, Can't power on <FRU Id>, its logical
switch is shut down
```

Probable cause Indicates that the specified field-replaceable unit (FRU) cannot be powered on because the associated logical switch is shut down.

Recommended action Start the associated logical switch.

Severity WARNING

EM-1045

Message

```
<timestamp>, [EM-1045], <sequence-number>,, WARNING,
<system-name>, <FRU Id> is being powered <new state>.
```

Probable cause Indicates that an automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. If new_state is On, a port blade is being powered on because more power is available (either a power supply was inserted or a port blade was removed or powered down). If new_state is Off, a port blade has been powered down because a power supply has been faulted, because it is indicating a predicted failure. If new_state is Down (not enough power), a newly inserted port blade was not powered on because there was not enough power available.

Recommended action For the ED-48000B, when there are no intelligent (AP) port blades installed, two power supplies are sufficient for redundancy; however, when one or more AP blades have been installed, four power supplies are required for complete redundancy.

Severity WARNING

EM-1046

Message

```
<timestamp>, [EM-1046], <sequence-number>,, WARNING,
<system-name>, Sysctrl reports error status for blade ID
<id value> for the blade in slot <slot number> <blade
incompatibility type: platform, backplane, or switch
configuration>
```

Probable cause Indicates that the blade specified is incompatible.

Recommended action If the blade ID listed is not correct, then the field-replaceable unit (FRU) header for the blade is corrupted and the blade must be

replaced. If the reason is due to *platform*, the blade ID listed is not supported for that platform (CP) type. Remove the blade from the chassis. If the reason is due to *backplane*, the CP type (CP256) is not supported on that chassis (backplane revision D2), remove the blade from the chassis.

If the reason is *switch configuration*, the blade's logical switch configuration is not correct. Run the **lscfg** command to correct the switch or port configuration for the ports on that blade.

Severity WARNING

EM-1047

Message

```
<timestamp>, [EM-1047], <sequence-number>,, INFO,
<system-name>, CP in slot <slot number> not faulty, CP
ERROR deasserted.
```

Probable cause Indicates that the control processor (CP) is no longer faulted. This message usually follows EM-1033. The new standby CP is in the process of rebooting and has turned off the CP_ERR signal.

Recommended action No action is required.

Severity INFO

EM-1048

Message

```
<timestamp>, [EM-1048], <sequence-number>,, INFO,
<system-name>, <FRU Id> I2C access recovered: state
<current state>
```

Probable cause Indicates that the I2C bus problems have been resolved and I2C access to the field-replaceable unit (FRU) has become available again.

Recommended action The EM-1029 error can be a transitory error; if the problem resolves, the EM-1048 message is displayed.

Severity INFO

EM-1049

Message

```
<timestamp>, [EM-1049], <sequence-number>,, INFO,
<system-name>, FRU <FRU Id> insertion detected.
```

Probable cause

Indicates that a field-replaceable unit (FRU) of the type and location specified by the FRU ID was detected as having been inserted into the chassis.

Recommended action

No action is required.

Severity

INFO

EM-1050

Message

```
<timestamp>, [EM-1050], <sequence-number>,, INFO,
<system-name>, FRU <FRU Id> removal detected.
```

Probable cause

Indicates that a field-replaceable unit (FRU) of the specified type and location was removed from the chassis.

Recommended action

Verify that the FRU was intended to be removed. Replace the FRU as soon as possible.

Severity

INFO

EM-1051

Message

```
<timestamp>, [EM-1051], <sequence-number>,, INFO,
<system-name>, <FRU Id>: Inconsistency detected, FRU
re-initialized.
```

Probable cause

Indicates that an inconsistent state was found in the field-replaceable unit (FRU). This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized and traffic might have been disrupted.

Recommended action

No action is required.

Severity

INFO

EM-1055

Message

```
<timestamp>, [EM-1055], <sequence-number>,, WARNING,
<system-name>, <FRU Id>: Port media incompatible. Reason:
<Reason for incompatibility>
```

Probable cause

Indicates that an incompatible port media is detected.

The possible causes are:

- The port media is not capable of running at the configured port speed.
- The port media generates too much heat to be used in the slot.

Recommended action

Verify that the media can be run at the configured port speed.

If the port media is extended long wavelength, move it to a port that can support the heat generated.

Severity

WARNING

EM-1056

Message

```
<timestamp>, [EM-1056], <sequence-number>,, WARNING,
<system-name>, <FRU Id>: Port faulted. Reason: <Reason
code for the fault>.
```

Probable cause

Indicates a faulty port media is detected. The reason code for this message is for internal use only. This message is valid for only the DS-4100B, DS-4900B, DS-5000B, MP-7500B, and AP-7600B.

Recommended action

Replace the defective small form-factor pluggable (SFP).

Severity

WARNING

EM-1057

Message

```
<timestamp>, [EM-1057], <sequence-number>,, WARNING,
<system-name>, Blade:<Slot Id> is getting reset:<Fault
reason>.
```

Probable cause The blade is automatically reset due to known resetable transient errors, such as an application-specific integrated circuit (ASIC) parity error.

Recommended action No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

Severity WARNING

EM-1058

Message

```
<timestamp>, [EM-1058], <sequence-number>,, WARNING,
<system-name>, Switch gets reset:<Fault reason>
```

Probable cause The switch is automatically reset due to known resetable transient errors, such as an application-specific integrated circuit (ASIC) parity. error.

Recommended action No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

Severity WARNING

EM-1059

Message

```
<timestamp>, [EM-1059], <sequence-number>, FFDC,
CRITICAL, <system-name>, Incompatible unit in <FRU Id>
faulted.
```

Probable cause Indicates that a field-replaceable unit (FRU) inserted in the specified slot is not compatible with the switch software. The blade will not be used.

Recommended action Replace the blade. Make sure the replacement is compatible with your switch type.

Severity CRITICAL

EM-1060

Message

```
<timestamp>, [EM-1060], <sequence-number>,, WARNING,
<system-name>, Stopping synchronization of the system due
to blade incompatibility with software version on standby
CP.
```

Probable cause

A blade in the system is not supported by the release on the standby control processor (CP).

Recommended action

Remove all blades of this type or upgrade your standby CP. Once an appropriate action is taken, this CP must be rebooted or **haSyncStart** must be run successfully. Until this is done, the system will remain out of synchronization.

Severity

WARNING

EM-1061

Message

```
<timestamp>, [EM-1061], <sequence-number>,, WARNING,
<system-name>, Synchronization halted. Remove all blades
of type <Blade Type Id> or upgrade your standby CP, then
reboot or run haSyncStart.
```

Probable cause

A blade in the system is not supported by the release on the standby control processor (CP).

Recommended action

Remove all blades of this type or upgrade your standby CP. Once an appropriate action is taken, this CP must be rebooted or **haSyncStart** must be run successfully. Until this is done, the system will remain out of synchronization.

Severity

WARNING

EM-1062

Message

```
<timestamp>, [EM-1062], <sequence-number>,, CRITICAL,
<system-name>, Blade in slot <Slot Id> faulted as it
exceeds the maximum support limit of <Limit> blades with
Blade ID <Blade Type Id> in the chassis.
```

Probable cause

Too many blades of a particular type are in the system.

Recommended action Remove the faulted blade.

Severity CRITICAL

EM-1063

Message

```
<timestamp>, [EM-1063], <sequence-number>,, CRITICAL,
<system-name>, Blade in slot <Slot Id> faulted because it
exceeds the maximum support limit of <Limit> blades with
Blade IDs <Applicable blade Type IDs> in the chassis.
```

Probable cause Too many blades of a set of particular types are in the system.

Recommended action Remove the faulted blade.

Severity CRITICAL

EM-1064

Message

```
<timestamp>, [EM-1064], <sequence-number>,, CRITICAL,
<system-name>, Blade:<slot ID> is being powered off
(based on user configuration) upon receiving a HW ASIC
ERROR, reason:<Fault reason>.
```

Probable cause The blade is powered off since a hardware (HW) application specific integrated circuit (ASIC) ERROR was detected, and the user has selected to power off the problem blade when such a condition occurred.

Recommended action Contact your EMC Customer Service representative.

Severity CRITICAL

EM-1065

Message

```
<timestamp>, [EM-1065], <sequence-number>,, CRITICAL,
<system-name>, SAS Virtualization Services are not
available due to incompatiblity between the FOS and SAS
versions <Slot number or blank for single board systems>.
```

Probable cause

The version of either the control processor firmware (CFOS) or the blade processor firmware (BFOS) is not compatible with the Storage Application Services (SAS) or other application firmware version(s).

Recommended action

Run the **firmwareDownload** command to upgrade the FOS firmware or the SAS firmware. Refer to the release notes for a compatible version of firmware.

Severity

CRITICAL

EM-1066

Message

```
<timestamp>, [EM-1066], <sequence-number>,, INFO,
<system-name>, SAS Virtualization Services are now
available <Slot number or blank for single board
systems>.
```

Probable cause

The previously incompatible Fabric OS or Storage Application Services (SAS) firmware have been upgraded and are now compatible.

Recommended action

No action is required.

Severity

INFO

EM-1067

Message

```
<timestamp>, [EM-1067], <sequence-number>,, WARNING,
<system-name>, Stopping synchronization of the system due
to version incompatibility with standby CP.
```

Probable Cause

Indicates that the firmware version on the standby CP is not compatible with this firmware version.

Recommended Action Run the **firmwareDownload** command to upgrade the firmware on the standby CP or downgrade the firmware on this CP.

Severity WARNING

EM-1068

Message

```
<timestamp>, [EM-1068], <sequence-number>,, ERROR,
<system-name>, High Availability Service Management
subsystem failed to respond.  A required component is not
operating.
```

Probable Cause Indicates that the HA subsystem has not returned a response within four minutes of the request from the Environmental Manager. It usually indicates that some component has not started properly or has terminated. The specific component that has failed might be indicated in other messages or debug data. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action Reboot or power cycle the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

EM-1069

Message

```
<timestamp>, [EM-1069], <sequence-number>,, INFO,
<system-name>, Slot <FRU slot number> is being powered
off.
```

Probable Cause Indicates a blade is being intentionally powered off.

Recommended Action No action is required.

Severity INFO

EM-1070

Message

```
<timestamp>, [EM-1070], <sequence-number>,, INFO,
<system-name>, Slot <FRU slot number> is being powered
on.
```

Probable Cause

Indicates a blade is being intentionally powered on.

Recommended Action

No action is required.

Severity

INFO

EM-2003

Message

```
<timestamp>, [EM-2003], <sequence-number>,, ERROR,
<system-name>, <Slot Id or Switch> has failed the POST
tests. FRU is being faulted.
```

Probable cause

Indicates that a field-replaceable unit (FRU) did not pass the Power On Self Tests. The ID will be *Switch* for non-bladed systems.

Recommended action

On bladed systems, try reseating the specified FRU.

On nonbladed switches, reboot or power cycle the switch.

If the problem persists:

- Run the **systemVerification** command to verify that the switch does not have hardware problems.
- On bladed systems, replace the specified FRU, otherwise replace the switch.

Severity

ERROR

17

ESS System Messages

This chapter contains information on the following ESS system messages.

- ESS-1001 212
- ESS-1002 212
- ESS-1003 213
- ESS-1004 213
- ESS-1005 214

ESS-1001

Message

```
<timestamp>, [ESS-1001], <sequence-number>,, WARNING,
<system-name>, A few switches in the fabric do not
support the Coordinated HotCode protocol.
```

Probable Cause

One or more switches in the fabric do not support the Coordinated HotCode protocol. Continuing with the firmware download may cause data traffic disruption.

Recommended Action

Discontinue the firmware download, identify the downlevel switch or switches that do not support the Coordinated HotCode protocol, and upgrade the downlevel switches. Then, restart the firmware download on this switch. Note that upgrading a downlevel switch in a mixed interop fabric may still cause data traffic disruption.

Severity

WARNING

ESS-1002

Message

```
<timestamp>, [ESS-1002], <sequence-number>,, WARNING,
<system-name>, The pause message is rejected by the
domain <domain id>.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

Recommended Action

No action is required.

Severity

WARNING

ESS-1003

Message

```
<timestamp>, [ESS-1003], <sequence-number>,, WARNING,
<system-name>, The pause retry count is exhausted for the
domain <domain id>.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action

No action is required.

Severity

WARNING

ESS-1004

Message

```
<timestamp>, [ESS-1004], <sequence-number>,, WARNING,
<system-name>, The resume message is rejected by the
domain <domain id>.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric has rejected the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected resume message.

Recommended Action

No action is required.

Severity

WARNING

ESS-1005

Message

```
<timestamp>, [ESS-1005], <sequence-number>,, WARNING,
<system-name>, The resume retry count is exhausted for
the domain <domain id>.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action

No action is required.

Severity

WARNING

18

EVMD System Messages

This chapter contains information on the following EVMD message:

- EVMD-1001 216

EVMD-1001

Message

```
<timestamp>, [EVMD-1001], <sequence-number>,, WARNING,
<system-name>, Event could not be sent to remote proxy. =
<Remote proxy switch id.>
```

Probable cause

The event could not be sent to the remote proxy because the remote proxy switch cannot be reached through in-band.

Recommended action

Make sure that the specified remote domain is present in the fabric.

Severity

WARNING

19

FABR System Messages

This chapter contains information on the following FABR messages:

- FABR-1001 219
- FABR-1002 219
- FABR-1003 219
- FABR-1004 220
- FABR-1005 220
- FABR-1006 221
- FABR-1007 221
- FABR-1008 222
- FABR-1009 222
- FABR-1010 223
- FABR-1011 223
- FABR-1012 223
- FABR-1013 224
- FABR-1014 224
- FABR-1015 225
- FABR-1016 225
- FABR-1017 226
- FABR-1018 226
- FABR-1019 226
- FABR-1020 227
- FABR-1021 227
- FABR-1022 228
- FABR-1023 228
- FABR-1024 229
- FABR-1029 229
- FABR-1030 230
- FABR-1031 230
- FABR-1032 231

- FABR-1034 231
- FABR-1035 231
- FABR-1036 232
- FABR-1037 232
- FABR-1038 233
- FABR-1039 233
- FABR-1040 233
- FABR-1041 234
- FABR-1043 234
- FABR-1044 234
- FABR-1045 235
- FABR-1046 235

FABR-1001

Message

```
<timestamp>, [FABR-1001], <sequence-number>,, WARNING,
<system-name>, port <port number>, <segmentation reason>.
```

Probable Cause

Indicates that the specified switch port is isolated because of a segmentation due to mismatched configuration parameters.

Recommended Action

Based on the segmentation reason displayed within the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the **configure** command to modify the appropriate switch parameters on both the local and remote switch.

Severity

WARNING

FABR-1002

Message

```
<timestamp>, [FABR-1002], <sequence-number>,, WARNING,
<system-name>, fabGaid: no free multicast alias IDs.
```

Probable Cause

Indicates that the fabric does not have any available multicast alias IDs to assign to the alias server.

Recommended Action

Verify alias IDs using the **fabricShow** command on the principal switch.

Severity

WARNING

FABR-1003

Message

```
<timestamp>, [FABR-1003], <sequence-number>,, WARNING,
<system-name>, port <port number>: ILS <command> bad size
<payload size>, wanted <expected payload size>.
```

Probable Cause

Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent an invalid sized payload.

Recommended Action

Investigate the neighbor switch for problems. Run the **errShow** command on the neighbor switch to view the error log for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting ports.

Run the **fabStateShow** command on both the receiving and transmitting switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1004

Message

```
<timestamp>, [FABR-1004], <sequence-number>,, WARNING,
<system-name>, port: <port number>, req iu: 0x<address of
IU request sent>, state: 0x<command sent>, resp iu:
0x<address of response IU received>, state 0x<response IU
state>, <additional description>.
```

Probable Cause Indicates that the information unit response was invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

Recommended Action If this message is due to a one-time event because of the incoming data, the system will discard the frame. If it is due to problems with the kernel, the system will recover by performing a failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1005

Message

```
<timestamp>, [FABR-1005], <sequence-number>,, WARNING,
<system-name>, <command sent>: port <port number>: status
0x<reason for failure> (<description of failure reason>)
xid = 0x<exchange ID of command>.
```

Probable Cause Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

Recommended Action No action is required; this message is often transitory.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1006

Message

```
<timestamp>, [FABR-1006], <sequence-number>,, WARNING,
<system-name>, Node free error, caller: <error
description>.
```

Probable Cause Indicates that the Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1007

Message

```
<timestamp>, [FABR-1007], <sequence-number>,, WARNING,
<system-name>, IU free error, caller: <function
attempting to de-allocate IU>.
```

Probable Cause Indicates that a failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1008

Message `<timestamp>, [FABR-1008], <sequence-number>,, WARNING, <system-name>, <error description>.`

Probable Cause Indicates that errors occurred during the request domain ID state; the information unit (IU) cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with the Fabric OS. The error descriptions are as follows:

- FAB RDI: Cannot allocate IU
- FAB RDI: Cannot send IU

Recommended Action No action is required if the message appears with the FABR_1005 message.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1009

Message `<timestamp>, [FABR-1009], <sequence-number>,, WARNING, <system-name>, <error description>.`

Probable Cause Indicates that errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty exchange fabric parameter (EFP) type. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The fabric daemon will discard the EFP. The system will recover through the EFP retrial process.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1010

Message `<timestamp>, [FABR-1010], <sequence-number>,, WARNING, <system-name>, <error description>.`

Probable Cause Indicates that the errors occurred while cleaning up the request domain ID (RDI). The error description provides further details. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1011

Message `<timestamp>, [FABR-1011], <sequence-number>, FFDC, ERROR, <system-name>, <error description>.`

Probable Cause Indicates that the Fabric OS is unable to inform the Fabric OS State Synchronization Management module (FSSME) that the fabric is stable or unstable. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

FABR-1012

Message `<timestamp>, [FABR-1012], <sequence-number>,, WARNING, <system-name>, <function stream>: no such type, <invalid type>.`

Probable Cause Indicates that the fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The fabric daemon will take proper action to recover from the error.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FABR-1013

Message

```
<timestamp>, [FABR-1013], <sequence-number>, FFDC,
CRITICAL, <system-name>, No Memory: pid=<fabric process
id> file=<source file name> line=<line number within the
source file>.
```

Probable Cause Indicates that there is not enough memory in the switch for the fabric module to allocate. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The system will recover by failing over to the standby CP.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity CRITICAL

FABR-1014

Message

```
<timestamp>, [FABR-1014], <sequence-number>, FFDC, ERROR,
<system-name>, Port <port number> Disabled: Insistent
Domain ID <Domain ID> could not be obtained. Principal
Assigned Domain ID = <Domain ID>
```

Probable Cause Indicates that the specified port received an request domain ID (RDI) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). Fibre connectivity (FICON) mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action Run the **configShow** command to view the fabric.ididmode. A 0 means the IDID mode is disabled; a 1 means it is enabled.

Set the switch to insistent domain ID mode. This mode is set under the **configure** command or in Web Tools on the **Switch Admin > configure** window.

Severity ERROR

FABR-1015

Message

```
<timestamp>, [FABR-1015], <sequence-number>, FFDC, ERROR,
<system-name>, FICON Insistent DID max retry exceeded:
All E-Ports will be disabled. Switch is isolated.
```

Probable Cause Indicates that the application exceeded request domain ID (RDI) requests for the insistent domain ID. All E_Ports are disabled, isolating the specified switch from the fabric.

Recommended Action Verify that the insistent domain ID is unique in the fabric and then reenable the E_Ports. Run the **fabricShow** command to view the domain IDs across the fabric and the **configure** command to change the insistent domain ID mode.

Severity ERROR

FABR-1016

Message

```
<timestamp>, [FABR-1016], <sequence-number>,, WARNING,
<system-name>, ficonMode is enabled.
```

Probable Cause Indicates that FICON mode is enabled on the switch through a user interface command.

Recommended Action No action is required.

Severity WARNING

FABR-1017

Message

```
<timestamp>, [FABR-1017], <sequence-number>,, WARNING,
<system-name>, ficonMode is disabled.
```

Probable Cause

Indicates that FICON mode is disabled on the switch through a user interface command.

Recommended Action

No action is required.

Severity

WARNING

FABR-1018

Message

```
<timestamp>, [FABR-1018], <sequence-number>,, WARNING,
<system-name>, PSS principal failed (<reason for not
becoming the principal switch>: <WWN of new principal
switch>).
```

Probable Cause

Indicates that a failure occurred when trying to set the principal switch using the **fabricPrincipal** command. The message notifies the user that the switch failed to become the principal switch because either:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower world wide name (WWN).

Recommended Action

Make sure that no other switches are configured as the principal switch. Force a fabric rebuild by using the **switchDisable** and **switchEnable** commands.

Severity

WARNING

FABR-1019

Message

```
<timestamp>, [FABR-1019], <sequence-number>, FFDC,
CRITICAL, <system-name>, Critical fabric size (<current
domains>) exceeds supported configuration (<supported
domains>).
```

Probable Cause Indicates that this switch is a value-line switch and has exceeded the limited fabric size: that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size has exceeded this specified limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your EMC account representative to obtain a full fabric license.

Severity CRITICAL

FABR-1020

Message

```
<timestamp>, [FABR-1020], <sequence-number>, FFDC,
CRITICAL, <system-name>, Web Tools will be disabled in
<days> days <hours> hours and <minutes> minutes.
```

Probable Cause Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days left in the grace period. After this time, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your EMC account representative to obtain a full fabric license.

Severity CRITICAL

FABR-1021

Message

```
<timestamp>, [FABR-1021], <sequence-number>, FFDC,
CRITICAL, <system-name>, Web Tools is disabled.
```

Probable Cause Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period has expired and Web Tools has been disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your EMC account representative to obtain a full fabric license.

Severity CRITICAL

FABR-1022

Message `<timestamp>, [FABR-1022], <sequence-number>, FFDC, CRITICAL, <system-name>, Fabric size (<actual domains>) exceeds supported configuration (<supported domains>). Fabric limit timer (<type>) started from <grace period in seconds>.`

Probable Cause Indicates that the fabric size has exceeded the value-line limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your EMC account representative to obtain a full fabric license.

Severity CRITICAL

FABR-1023

Message `<timestamp>, [FABR-1023], <sequence-number>,, INFO, <system-name>, Fabric size is within supported configuration (<supporteddomains>). Fabric limit timer (<type>) stopped at <grace period in seconds>.`

Probable Cause Indicates that the fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

Recommended Action No action is required.

Severity INFO

FABR-1024

Message

```
<timestamp>, [FABR-1024], <sequence-number>,, INFO,
<system-name>, Initializing fabric size limit timer
<grace period>
```

Probable Cause

Indicates that the fabric size has exceeded the limit set by your value-line switches. Value-line switches have a limited fabric size: a specified limit to the number of domains. This value is defined by your specific value-line license key. The fabric size has exceeded this specified limit. The grace-period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action

Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your EMC account representative to obtain a full fabric license.

Severity

INFO

FABR-1029

Message

```
<timestamp>, [FABR-1029], <sequence-number>,, INFO,
<system-name>, Port <port number> negotiated <flow
control mode description> (mode = <received flow control
mode>).
```

Probable Cause

Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. There are three types of flow control modes:

- VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.

- DUAL_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of exchange link parameter (ELP) exchange. This mode also uses the R_RDY primitive for flow control.

Recommended Action No action is required.

Severity INFO

FABR-1030

Message `<timestamp>, [FABR-1030], <sequence-number>,, INFO, <system-name>, fabric: Domain <new domain ID> (was <old domain ID>).`

Probable Cause Indicates that the domain ID has changed as specified.

Recommended Action No action is required.

Severity INFO

FABR-1031

Message `<timestamp>, [FABR-1031], <sequence-number>, FFDC, WARNING, <system-name>, Maximum number of retries sending ILS from port <port number> exceeded.`

Probable Cause Indicates that fabric exhausted the maximum number of retries sending internal link service (ILS) to the iswitchd demon on the specified E_Port.

Recommended Action Run the **top** command to see if iswitchd is extremely busy or if another process is using excessive CPU resources.

Severity WARNING

FABR-1032

Message

```
<timestamp>, [FABR-1032], <sequence-number>, FFDC,
WARNING, <system-name>, Remote switch with domain ID
<domain ID>and switchname <switchname>running an
unsupported FOS version v2.x has joined the fabric.
```

Probable Cause

Indicates that a switch with an unsupported Fabric OS version 2.x has joined the fabric.

Recommended Action

Remove the switch with the unsupported Fabric OS version 2.x from the fabric.

FABR-1034

Message

```
<timestamp>, [FABR-1034], <sequence-number>,, INFO,
<system-name>, Area <Area that has already been acquired>
have been acquired by port <Port that has already
acquired the area>. Persistently disabling port <Port
that is being disabled>.
```

Probable Cause

Trunk Area is not enabled on a port, therefore another port can not use the same area. The port was persistently disabled.

Recommended Action

You must move the cable to a port area that is not in use, or disable the Trunk Area. The port must be manually persistently enabled.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information.

Severity

INFO

FABR-1035

Message

```
<timestamp>, [FABR-1035], <sequence-number>,, INFO,
<system-name>, Slave area <Area that does not match
Master port's area> does not match Master port <Master
port>. Persistently disabling port <Port that is being
disabled>.
```

Probable Cause

The Slave port's Trunk Area differs with that of the Master port. The port was persistently disabled.

Recommended Action You must move the cable to a port to match the same Master Trunk Area, or disable the Trunk Area. The port must be manually persistently enabled.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information.

Severity INFO

FABR-1036

Message

```
<timestamp>, [FABR-1036], <sequence-number>,, INFO,
<system-name>, F_port trunks are only allowed on Trunk
Area enabled port. Persistently disabling port <Port that
is being disabled>.
```

Probable Cause When a port on a switch is Trunk Area enabled, it only allows an F_Port to connect.

Recommended Action Move the cable to a port that does not have Trunk Area enabled. The port must be manually persistently enabled.

Severity INFO

FABR-1037

Message

```
<timestamp>, [FABR-1037], <sequence-number>,, INFO,
<system-name>, Port configuration incompatible with Trunk
Area enabled port. Persistently disabling port <Port that
is being disabled>.
```

Probable Cause When the port attempts to go online, the switch finds the Trunk Area enabled with an incompatible port configuration such as long distance, port mirror, fast write, or EX_Port. The port was persistently disabled.

Recommended Action Check the port configuration to disable long distance, port mirror, fast write or EX_Port. The port must be manually persistently enabled.

Severity INFO

FABR-1038

Message

```
<timestamp>, [FABR-1038], <sequence-number>,, INFO,
<system-name>, Trunking license not present with F port
trunking enabled. Persistently disabling port <Port that
is being disabled>.
```

Probable Cause Trunking license is not present when F_Port trunking is enabled. The port was persistently disabled.

Recommended Action Install a trunking license or disable F_Port trunking over the port. The port must be manually persistently enabled.

Severity INFO

FABR-1039

Message

```
<timestamp>, [FABR-1039], <sequence-number>,, WARNING,
<system-name>, Invalid domain id zero received from
principal switch (domain id=<Principal domain id>).
```

Probable Cause Indicates an invalid domain id of zero has been received.

Recommended Action Check the domain ID of the principal switch, and run the **configure** command to set it to a non-conflicting, non-zero ID.

Severity WARNING

FABR-1040

Message

```
<timestamp>, [FABR-1040], <sequence-number>,, INFO,
<system-name>, Speed is not 2g,4g or 8g with F_port
trunking enabled. Persistently disabling port <Port that
is being disabled>.
```

Probable Cause Indicates that the speed is not compatible for F_Port trunks.

Recommended Action Change the speed for the port or disable F_Port trunking on the port.

Severity INFO

FABR-1041

Message

```
<timestamp>, [FABR-1041], <sequence-number>,, ERROR,
<system-name>, Port <Port that is being disabled> is
disabled due to trunk protocol error.
```

Probable Cause

Indicates that a link reset was received before the completion of the trunking protocol on the port.

Recommended Action

Enable the port by running **portEnable** command. The port may recover by re-initialization of the link.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

FABR-1043

Message

```
<timestamp>, [FABR-1043], <sequence-number>,, ERROR,
<system-name>, Detected Fabric ID conflict with remote
(not neighbor) switch <Switchname> (domain <Domain ID>),
FID <Fabric ID>. No local E-ports disabled.
```

Probable Cause

Indicates that the remote switch has a Fabric ID conflict with the local switch, but no ports are disabled because the remote switch is not adjacent to the local switch.

Recommended Action

Make sure that all the switches in the fabric have the same Fabric ID or upgrade the switch firmware to a Virtual Fabric-capable firmware version.

Severity

ERROR

FABR-1044

Message

```
<timestamp>, [FABR-1044], <sequence-number>,, ERROR,
<system-name>, Detected Fabric ID conflict with neighbor
switch <Switchname> (domain <Domain ID>), FID <Fabric
ID>.  E-ports (<Number of E-ports disabled>) connected to
the switch are disabled.
```

Probable Cause Indicates that the neighbor switch has a Fabric ID conflict with the local switch. All E_Ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same Fabric ID or upgrade the switch firmware to a Virtual Fabric-capable firmware version.

Severity ERROR

FABR-1045

Message

```
<timestamp>, [FABR-1045], <sequence-number>,, ERROR,
<system-name>, <Text>Detected Base Switch conflict with
remote (not neighbor) switch <Switchname> (domain <Domain
ID>), BS <Base Switch Mode>. No local E-ports disabled.
```

Probable Cause Indicates that the remote switch has a Base Switch attribute conflict with the local switch, but no ports are disabled because the remote switch is not adjacent to the local switch.

Recommended Action Make sure that all the switches in the fabric have the same Base Switch attribute or disable Virtual Fabric mode for the conflicting switch using the **fosconfig** command.

Severity ERROR

FABR-1046

Message

```
<timestamp>, [FABR-1046], <sequence-number>,, ERROR,
<system-name>, Detected Base Switch conflict with
neighbor switch <Switchname> (domain <Domain ID>), BS
<Base Switch Mode>.  E-ports (<Number of E-ports
disabled>) connected to the switch are disabled.
```

Probable Cause Indicates that the remote switch has a Base Switch attribute conflict with the local switch. All the E_Ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same Base Switch attribute or upgrade the switch firmware to a Virtual Fabric-capable firmware version.

Severity ERROR

20

FABS System Messages

This chapter contains information on the following FABS messages:

- FABS-1001 238
- FABS-1002 238
- FABS-1004 238
- FABS-1005 239
- FABS-1006 239
- FABS-1007 240
- FABS-1008 240
- FABS-1009 241
- FABS-1010 241
- FABS-1011 241
- FABS-1012 242
- FABS-1013 242
- FABS-1014 243
- FABS-1015 243

FABS-1001

Message

```
<timestamp>, [FABS-1001], <sequence-number>,, FFDC,
CRITICAL, <system-name>, <Function name> <Description of
memory need>
```

Probable cause

Indicates that the system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. *Description of memory need* indicates how much memory was being requested. The value could be any whole number.

Recommended action

Reboot or power cycle the switch.

Severity

CRITICAL

FABS-1002

Message

```
<timestamp>, [FABS-1002], <sequence-number>,, WARNING,
<system-name>, <Function name> <Description of problem>
```

Probable cause

Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

Recommended action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1004

Message

```
<timestamp>, [FABS-1004], <sequence-number>,, WARNING,
<system-name>, <Function name and description of problem>
process <Process ID number> (<Current command name>)
<Pending signal number>
```

Probable cause

Indicates that an operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

Recommended action Reboot or power cycle the switch.

Severity WARNING

FABS-1005

Message

```
<timestamp>, [FABS-1005], <sequence-number>,, WARNING,
<system-name>, <Function name and description of problem>
(<ID type>= <ID number>)
```

Probable cause Indicates that an unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The possible values for *function name and description of problem* are:

fabsys_write: Unsupported write operation: process xxx

where "xxx" is the process ID (PID), which could be any whole number.

Recommended action Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems).

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1006

Message

```
<timestamp>, [FABS-1006], <sequence-number>,, WARNING,
<system-name>, <Function name and description of
problem>: object <object type id> unit <slot>
```

Probable cause Indicates that there is no device in the slot with the specified object type ID in the system module record. This could indicate a serious Fabric OS data problem on the switch. The possible values for *function name and description of problem* are:

- setSoftState: Bad object
- setSoftState: Invalid type or unit
- media_sync: Media oid mapping failed
- fabsys_media_i2c_op: Media oid mapping failed

- fabsys_media_i2c_op: obj is not media type
- media_class_hndlr: failed sending media state to blade driver

Recommended action If the message is isolated, monitor the error messages on the switch. If the error is repetitive or if the fabric failed, fail over or reboot the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1007

Message

```
<timestamp>, [FABS-1007], <sequence-number>,, WARNING,
<system-name>, <Function name>: Media state is invalid -
status=<Status value>
```

Probable cause Indicates that the Fabric OS has detected an invalid value in an object's status field. This is usually an internal Fabric OS problem or file corruption.

Recommended action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1008

Message

```
<timestamp>, [FABS-1008], <sequence-number>,, WARNING,
<system-name>, <Function name>: Media oid mapping failed
```

Probable cause Indicates that the Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended action Reboot or power cycle the switch.

Severity WARNING

FABS-1009

Message

```
<timestamp>, [FABS-1009], <sequence-number>,, WARNING,
<system-name>, <Function name>: type is not media
```

Probable cause

Indicates that the Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended action

Reboot or power cycle the switch.

Severity

WARNING

FABS-1010

Message

```
<timestamp>, [FABS-1010], <sequence-number>,, WARNING,
<system-name>, <Function name>: Wrong media_event <Event
number>
```

Probable cause

Indicates that the Fabric OS detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

Recommended action

Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

WARNING

FABS-1011

Message

```
<timestamp>, [FABS-1011], <sequence-number>,, ERROR,
<system-name>, <Method name>[<Method tag number>]:Invalid
input state 0x<Input state code>
```

Probable cause

An unrecognized state code was used in an internal Fabric OS message for a FRU.

Recommended action

Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity ERROR

FABS-1012

Message

```
<timestamp>, [FABS-1012], <sequence-number>,, ERROR,
<system-name>, <Method name>[<Method tag number>]:FRU
state transition failed. Current state 0x<Current state
of FRU> Requested state 0x<Requested new state of FRU>
err 0x<Error code>
```

Probable cause A FRU could not be transitioned to the requested state. This is usually an internal Fabric OS problem.

Recommended action Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity ERROR

FABS-1013

Message

```
<timestamp>, [FABS-1013], <sequence-number>,, ERROR,
<system-name>, <Method name>[<Method tag number>]:Unknown
blade type 0x<Blade type>
```

Probable cause An unrecognized type of blade has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the blade may not be supported by this platform or Fabric OS version.

Recommended action Verify that the blade is valid for use in this system and this version of Fabric OS.

Try reseating the blade.

If this is a valid blade and reseating does not fix the problem, then replace the blade.

Severity ERROR

FABS-1014

Message

```
<timestamp>, [FABS-1014], <sequence-number>,, ERROR,
<system-name>, <Method name>[<Method tag number>]:Unknown
FRU type 0x<FRU Object type>
```

Probable cause

An unrecognized type of FRU has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Fabric OS version.

Recommended action

Verify that the FRU is valid for use in this system and this version of Fabric OS.

Try reseating the FRU.

If this is a valid FRU and reseating doesn't help, then replace the FRU.

Severity

ERROR

FABS-1015

Message

```
<timestamp>, [FABS-1015], <sequence-number>,, ERROR,
<system-name>, <Method name>[<Method tag number>]:Request
to enable FRU type 0x<FRU Object type>, unit <Unit
number> failed. err code <Error code>
```

Probable cause

Indicates the specified FRU could not be enabled. This is usually an internal Fabric OS problem.

Recommended action

Try removing and reinserting the FRU.

Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity

ERROR

21

FBC System Messages

This chapter contains information on the following FBC message:

- FBC-1001 246

FBC-1001

Message

```
<timestamp>, [FBC-1001], <sequence-number>,, ERROR,
<system-name>, Firmware version on AP blade is
incompatible with that on the CP.
```

Probable cause

The CP determined that the version of firmware running on the AP blade is not compatible with the version of firmware running on the CP. The AP and CP blades cannot communicate.

Recommended action

The problem can be corrected by changing the version of firmware on the CP or AP blades. The firmware version on the CP blade can be changed by running the **firmwareDownload** command. Refer to the release notes to determine whether a non-disruptive **firmwareDownload** is supported between the versions. As the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If required, replace the AP blade.

Severity

ERROR

22

FCIP System Messages

This chapter contains information on the following FCIP messages:

- FCIP-1000 248
- FCIP-1001 248
- FCIP-1002 248
- FCIP-1003 249
- FCIP-1004 249

FCIP-1000

Message `<timestamp>, [FCIP-1000], <sequence-number>, FFDC, ERROR, <system-name>, <command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>`

Probable cause Indicates that the hardware is not responding to a command request; possibly because it is busy.

Recommended action Retry the command.

Severity ERROR

FCIP-1001

Message `<timestamp>, [FCIP-1001], <sequence-number>, FFDC, ERROR, <system-name>, FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.`

Probable cause Indicates that the FIPS failure has occured and requires faulting the blade or switch.

Recommended action Retry the command.

Severity ERROR

FCIP-1002

Message `<timestamp>, [FCIP-1002], <sequence-number>, INFO, CFG, <system-name>, An IPsec/IKE policy was added.`

Probable Cause Indicates that an IPsec/IKE policy was added and the config file was updated.

Recommended Action No action is required.

Severity INFO

FCIP-1003

Message

```
<timestamp>, [FCIP-1003], <sequence-number>, INFO, CFG,
<system-name>, An IPsec/IKE policy was deleted.
```

Probable Cause

Indicates that an IPsec/IKE policy was deleted and the config file was updated.

Recommended Action

No action is required.

Severity

INFO

FCIP-1004

Message

```
<timestamp>, [FCIP-1004], <sequence-number>, INFO, CFG,
<system-name>, Tape Read Pipelining is being disabled
slot (<slot number>) port (<user port index>) tunnel
(<The configured tunnel ID (0-7)>).
```

Probable Cause

Indicates that the FOS version on the remote end of the tunnel does not support Tape Read Pipelining.

Recommended Action

No action is required.

Severity

INFO

23

FCMC System Messages

This chapter contains information on the following FCMC message:

- FCMC-1001 252

FCMC-1001

Message

```
<timestamp>, [FCMC-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, System is low on memory and has
failed to allocate new memory.
```

Probable cause

Indicates that the switch is low on memory and failed to allocate new memory for an information unit (IU).

Recommended action

A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

Severity

CRITICAL

24

FCPD System Messages

This chapter contains information on the following FCPD messages:

- FCPD-1001 254
- FCPD-1002 254
- FCPD-1003 255

FCPD-1001

Message

```
<timestamp>, [FCPD-1001], <sequence-number>,, WARNING,
<system-name>, Probing failed on <error string>.
```

Probable cause

Indicates that a fibre channel protocol (FCP) switch probed devices on a loop port, and the probing failed on the either the L_Port, AL_PA address, or the F_Port. For the AL_PA, the valid range is 00 through FF. The error string can be either:

- L_Port *port_number* ALPA *alpa_number*
- F_Port *port_number*

Recommended action

This can happen when the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

Severity

WARNING

FCPD-1002

Message

```
<timestamp>, [FCPD-1002], <sequence-number>,, WARNING,
<system-name>, port <port number>, bad R_CTL for fcp
probing: 0x<R_CTL value>
```

Probable cause

Indicates that the response frame received on the specified port for a inquiry request contains an invalid value in the routing control field.

Recommended action

This can happen only if the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

Severity

WARNING

FCPD-1003

Message

```
<timestamp>, [FCPD-1003], <sequence-number>,, INFO,
<system-name>, Probing failed on <error string> which is
possibly a private device which is not supported in this
port type
```

Probable cause

Private devices will not respond to the switch port login (PLOGI) during probing.

Recommended action

Switches and enterprise-class platforms capable of running Fabric OS 6.0 or higher do not support private loop devices. Contact your EMC Customer Service representative or refer to the latest version of the *EMC Support Matrix* for a list of other port types that support private devices for inclusion into the fabric.

Severity

INFO

25

FCPH System Messages

This chapter contains information on the following FCPH message:

- FCPH-1001 258
- FCPH-1002 258

FCPH-1001

Message

```
<timestamp>, [FCPH-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, <function>: <failed function
call> failed, out of memory condition
```

Probable cause

Indicates that the switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* can only be " fc_create". This function creates a Fibre Channel driver instance.

The *failed function call* is "kmalloc_wrapper failed". This function call is for kernel memory allocation.

Recommended action

A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over, and the standby CP will become the active CP.

Severity

CRITICAL

FCPH-1002

Message

```
<timestamp>, [FCPH-1002], <sequence-number>, FFDC,
WARNING, <system-name>, Port <Port Number> has been
disabled since switch requires authentication when device
authentication policy is set to ON.
```

Probable Cause

Indicates a device which does not support authentication has tried to log in to the switch when the device authentication policy is in ON status on the switch.

Recommended Action

Enable the authentication on the device or set the device authentication status to PASSIVE/OFF on the switch if it is not mandatory. Use the **authUtil** command to change the device authentication policy.

Severity

WARNING

26

FCR System Messages

This chapter contains information on the following FCR messages:

- FCR-1001 262
- FCR-1002 262
- FCR-1003 262
- FCR-1004 263
- FCR-1005 263
- FCR-1006 263
- FCR-1007 264
- FCR-1008 264
- FCR-1009 264
- FCR-1010 265
- FCR-1011 265
- FCR-1012 265
- FCR-1013 266
- FCR-1015 266
- FCR-1016 266
- FCR-1018 267
- FCR-1019 267
- FCR-1020 268
- FCR-1021 268
- FCR-1022 269
- FCR-1023 269
- FCR-1024 269
- FCR-1025 270
- FCR-1026 270
- FCR-1027 271
- FCR-1028 271
- FCR-1029 272

- FCR-1030 272
- FCR-1031 273
- FCR-1032 273
- FCR-1033 273
- FCR-1034 274
- FCR-1035 274
- FCR-1036 274
- FCR-1037 275
- FCR-1038 275
- FCR-1039 275
- FCR-1040 276
- FCR-1041 276
- FCR-1042 276
- FCR-1043 277
- FCR-1048 277
- FCR-1049 277
- FCR-1053 278
- FCR-1054 278
- FCR-1055 279
- FCR-1056 279
- FCR-1057 279
- FCR-1058 280
- FCR-1059 280
- FCR-1060 281
- FCR-1061 281
- FCR-1062 282
- FCR-1063 282
- FCR-1064 282
- FCR-1065 283
- FCR-1066 283
- FCR-1067 284
- FCR-1068 284
- FCR-1069 284
- FCR-1070 285
- FCR-1071 285
- FCR-1072 285
- FCR-1073 286
- FCR-1074 286
- FCR-1075 287
- FCR-1076 287
- FCR-1077 287
- FCR-1078 288
- FCR-1079 288

- FCR-1080 289
- FCR-1081 289
- FCR-1082 289
- FCR-1083 290
- FCR-1084 290
- FCR-1085 291
- FCR-1086 291
- FCR-1087 291
- FCR-1088 292
- FCR-1089 292

FCR-1001

Message `<timestamp>, [FCR-1001], <sequence-number>,, INFO, <system-name>, FC router proxy device in edge created at port <port number>.`

Probable Cause Indicates that a proxy device in the edge fabric has been imported at the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1002

Message `<timestamp>, [FCR-1002], <sequence-number>,, INFO, <system-name>, FC router proxy device in edge deleted at port <port number>.`

Probable Cause Indicates that a proxy device in the edge fabric has been deleted at the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1003

Message `<timestamp>, [FCR-1003], <sequence-number>,, INFO, <system-name>,FC router physical devices newly exported at port <port number>.`

Probable Cause Indicates that one or more physical devices have been newly exported through the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1004

Message

```
<timestamp>, [FCR-1004], <sequence-number>,, INFO,
<system-name>, FC router physical devices offline at port
<port number>.
```

Probable Cause

Indicates that one or more physical devices connected to the specified port have gone offline.

Recommended Action

Verify that the device(s) were intended to be taken offline.

If not, verify that the devices are functioning properly. Verify that all small form-factor pluggables (SFPs) are seated correctly. Check for faulty cables, deteriorated SFPs, or dirty connections. Replace the cables and SFPs if necessary.

Severity

INFO

FCR-1005

Message

```
<timestamp>, [FCR-1005], <sequence-number>,, INFO,
<system-name>, FC router LSAN zone device removed at port
<port number>.
```

Probable Cause

Indicates that a device is removed from the logical storage area network (LSAN) zone in the edge fabric.

Recommended Action

No action is required.

Severity

INFO

FCR-1006

Message

```
<timestamp>, [FCR-1006], <sequence-number>,, INFO,
<system-name>, FC router LSAN zone device added at port
<port number>.
```

Probable Cause

Indicates that a device is added to a logical storage area network (LSAN) zone in the edge fabric.

Recommended Action

No action is required.

Severity INFO

FCR-1007

Message `<timestamp>, [FCR-1007], <sequence-number>,, INFO, <system-name>, FC router LSAN zone deleted at port <port number>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone attached to the specified port was deleted from the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1008

Message `<timestamp>, [FCR-1008], <sequence-number>,, INFO, <system-name>, FC router LSAN zone created at port <port number>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone was created at the specified port in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1009

Message `<timestamp>, [FCR-1009], <sequence-number>,, INFO, <system-name>, FC router LSAN zone enabled at port <port number>: <enabled name>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone was enabled in the edge fabric attached to the specified port. The enabled LSAN zone configuration is listed.

Recommended Action No action is required.

Severity INFO

FCR-1010

Message `<timestamp>, [FCR-1010], <sequence-number>,, INFO, <system-name>, FC router LSAN zone disabled at port <port number>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone is disabled in the edge fabric attached to the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1011

Message `<timestamp>, [FCR-1011], <sequence-number>,, INFO, <system-name>, Remote LSAN zone updated in domain <domain ID>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone update was received from another domain.

Recommended Action No action is required.

Severity INFO

FCR-1012

Message `<timestamp>, [FCR-1012], <sequence-number>,, INFO, <system-name>, FC Router fabric build completed on port <port number>.`

Probable Cause Indicates that the fibre channel router has completed a fabric build at the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1013

Message `<timestamp>, [FCR-1013], <sequence-number>,, INFO, <system-name>, Phantom FSPF database exchange completed on port <port number>.`

Probable Cause Indicates that the specified EX_Port has completed the fabric shortest path first (FSFP) database exchange.

Recommended Action No action is required.

Severity INFO

FCR-1015

Message `<timestamp>, [FCR-1015], <sequence-number>,, INFO, <system-name>, New EX_Port or VEX_Port added on port <port number> in domain <domain ID>.`

Probable Cause Indicates that an EX _Port was created on the specified port in the specified domain.

Recommended Action No action is required.

Severity INFO

FCR-1016

Message `<timestamp>, [FCR-1016], <sequence-number>,, INFO, <system-name>, FCR fabric no longer reachable at port id <port number> fabric ID <fabric ID>.`

Probable Cause Indicates that a fabric is no longer accessible through the backbone fabric. This may be caused by a link or switch failure.

Recommended Action No action is required.

Severity INFO

FCR-1018

Message

```
<timestamp>, [FCR-1018], <sequence-number>,, ERROR,
<system-name>, FC router proxy device entries exhausted
on port <port number>.
```

Probable Cause

Indicates that the number of proxy devices is greater than allowed by the port resource.

Recommended Action

Remove excess logical storage area network (LSAN) zones or devices until the number of proxy devices exported is within the range allowed by the port resource. Use the **fcrResourceShow** command to view resources including LSAN zone resources, LSAN device resources, and proxy device port resources.

Use the **fcrProxyDevShow** command to view how many proxy devices are created in the fabric with the port resource problem.

LSAN zones are removed using standard zoning commands such as **zoneShow**, **zoneRemove**, **zoneDelete**, **cfgDelete**, and **cfgDisable** in the edge fabric. Proxy devices can be removed by zoning operations or by bringing physical devices offline. For example, disabling the port that a device is attached to, and then disconnecting the cable or disabling the device.

Severity

ERROR

FCR-1019

Message

```
<timestamp>, [FCR-1019], <sequence-number>,, ERROR,
<system-name>, EX or VEX port entries exhausted at port
<port number>.
```

Probable Cause

Indicates that the number of EX_Port or VEX_Port entries being created is greater than allowed by the port resource.

Recommended Action

EX_Port or VEX_Ports exceeding the range allowed by the port resource will be automatically disabled. Use the **fcrRouteShow** command to display the NR_Port limits.

Severity

ERROR

FCR-1020

Message

```
<timestamp>, [FCR-1020], <sequence-number>,, WARNING,
<system-name>, Local LSAN zone entries for FC router
exhausted; max limit: <LSAN zone limit>.
```

Probable Cause

Indicates that the number of logical storage area network (LSAN) zones created within a MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action

Remove excess LSAN zones so that the number of LSAN zones created is within the range of local database limitations.

To do that, perform the following steps:

1. Run **portDisable** to disable all the EX_Ports that got this error message.
2. Run **portDisable** to disable all the other EX_Ports on that FCR connected to the same edge fabrics the EX_Ports disabled in step 1 are connected to.
3. Use Zoning commands on the edge fabrics, to reduce the LSAN zone entries on the edge fabrics.
4. Run **portEnable** on each EX_Port, one at a time, to reenable the EX_Ports, and verify that this error is not reported again.

Severity

WARNING

FCR-1021

Message

```
<timestamp>, [FCR-1021], <sequence-number>,, WARNING,
<system-name>, Local LSAN device entries exhausted.
```

Probable Cause

Indicates that the number of devices created through logical storage area network (LSAN) zones within the MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action

Remove excess device entries within LSAN zones so that the number of devices is within the range of the local zone database limitations.

Severity

WARNING

FCR-1022

Message

```
<timestamp>, [FCR-1022], <sequence-number>,, ERROR,
<system-name>, Local proxy device slot entries exhausted.
```

Probable Cause

Indicates that the resources used to persistently store the proxy device slot to the remote world-wide name (WWN) have been consumed.

Recommended Action

Remove the proxy device slots by using the **fcrProxyConfig** command or limit proxy devices by removing logical storage area network (LSAN) zone entries.

Severity

ERROR

FCR-1023

Message

```
<timestamp>, [FCR-1023], <sequence-number>,, WARNING,
<system-name>, Local phantom port WWN entries exhausted.
```

Probable Cause

Indicates that the number of port world-wide names (WWNs) in use exceeds the local port WWN resources.

Recommended Action

Limit the number of port WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains). You can also limit the number of proxy devices for a translate domain (which limits the number of translate domain ports required) by limiting the devices specified in logical storage area network (LSAN) zones.

Severity

WARNING

FCR-1024

Message

```
<timestamp>, [FCR-1024], <sequence-number>,, WARNING,
<system-name>, Local LSAN zone <zone name> device
entries for edge LSAN exhausted.
```

Probable Cause

Indicates that the number of devices in a logical storage area network (LSAN) defined in the edge fabric exceeds the local LSAN zone database limitations.

Recommended Action Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

Severity WARNING

FCR-1025

Message

```
<timestamp>, [FCR-1025], <sequence-number>,, WARNING,
<system-name>, Local phantom node WWN entries exhausted.
```

Probable Cause Indicates that the number of node world-wide names (WWNs) detected to be in use exceeds the local node WWN resources.

Recommended Action Reduce the number of node WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains).

Severity WARNING

FCR-1026

Message

```
<timestamp>, [FCR-1026], <sequence-number>,, INFO,
<system-name>, In slot <slot number> Node WWN roll over.
```

Probable Cause Indicates that the node world-wide name (WWN) pool has rolled over in the specified slot, and WWN entries detected to not be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled then reenabled.

Severity INFO

FCR-1027

Message

```
<timestamp>, [FCR-1027], <sequence-number>,, INFO,
<system-name>, In slot <slot number> port WWN roll over.
```

Probable Cause

Indicates that the port world-wide name (WWN) pool has rolled over in the specified slot, and WWN entries detected to not be in use are reused as needed.

Recommended Action

It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port or VEX_Port connectivity should be disabled then re-enabled.

Severity

INFO

FCR-1028

Message

```
<timestamp>, [FCR-1028], <sequence-number>,, INFO,
<system-name>, In slot <slot number> node WWN pool 95
percent allocated.
```

Probable Cause

Indicates that the node world-wide name (WWN) pool is close to rollover in the specified slot, and that the WWN entries detected to not be in use will be reused as needed.

Recommended Action

It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port or VEX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled then reenabled.

Severity INFO

FCR-1029

Message `<timestamp>, [FCR-1029], <sequence-number>,, INFO, <system-name>, In slot <slot number> port WWN pool 95 percent allocated.`

Probable Cause Indicates that the Port world-wide name (WWN) pool has rolled over in the specified slot, and WWN entries detected to not be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled then reenabled.

Severity INFO

FCR-1030

Message `<timestamp>, [FCR-1030], <sequence-number>,, INFO, <system-name>, Physical device <device WWN> came online at fabric <fabric ID>.`

Probable Cause Indicates that the physical device world-wide name (WWN) came online in the specified fabric.

Recommended Action No action is required.

Severity INFO

FCR-1031

Message `<timestamp>, [FCR-1031], <sequence-number>,, INFO, <system-name>, Physical device <device WWN> went offline in fabric <fabric ID>.`

Probable Cause Indicates that the physical device world-wide name (WWN) went offline in the specified fabric.

Recommended Action No action is required.

Severity INFO

FCR-1032

Message `<timestamp>, [FCR-1032], <sequence-number>,, INFO, <system-name>, Edge fabric enabled security on port <port number> in fabric <fabric ID>.`

Probable Cause Indicates that Secure mode was turned on in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1033

Message `<timestamp>, [FCR-1033], <sequence-number>,, INFO, <system-name>, Edge fabric disabled security on port <port number> in fabric <fabric ID>.`

Probable Cause Indicates that Secure mode was turned off in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1034

Message `<timestamp>, [FCR-1034], <sequence-number>,, INFO, <system-name>, LSAN zone added in backbone fabric.`

Probable Cause Indicates that a new logical storage area network (LSAN) zone was added to the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1035

Message `<timestamp>, [FCR-1035], <sequence-number>,, INFO, <system-name>, LSAN zone device added in the backbone fabric.`

Probable Cause Indicates that a new device was added to a logical storage area network (LSAN) zone in the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1036

Message `<timestamp>, [FCR-1036], <sequence-number>,, INFO, <system-name>, LSAN zone <zone name> enabled in the backbone fabric.`

Probable Cause Indicates that the specified logical storage area network (LSAN) zone was enabled in the backbone fabric. The enabled LSAN zone configuration is listed.

Recommended Action No action is required.

Severity INFO

FCR-1037

Message `<timestamp>, [FCR-1037], <sequence-number>,, INFO, <system-name>, LSAN zone disabled in the backbone fabric.`

Probable Cause Indicates that a logical storage area network (LSAN) zone is disabled in the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1038

Message `<timestamp>, [FCR-1038], <sequence-number>,, WARNING, <system-name>, Total zone entries exceeded local fabric limits by <overflow> entries, in zone: <zone name>, zone limit: <LSAN zone limit>.`

Probable Cause Indicates that the number of cfg/zone/alias entries created in a local fabric is greater than the local switch's zone database limitations.

Recommended Action Remove excess cfg/zone/alias entries so that the number of logical storage area network (LSAN) zones created is within the range of the local database limitations.

Severity WARNING

FCR-1039

Message `<timestamp>, [FCR-1039], <sequence-number>,, INFO, <system-name>, Local LSAN zone <zone name> device entries for backbone LSAN exhausted.`

Probable Cause Indicates that the number of devices in the specified logical storage area network (LSAN) defined in the backbone fabric is greater than allowed by the local LSAN zone database limitations.

Recommended Action Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

Severity INFO

FCR-1040

Message `<timestamp>, [FCR-1040], <sequence-number>,, INFO, <system-name>, Proxy device deleted in the backbone fabric.`

Probable Cause Indicates that a proxy device created in the backbone fabric was deleted.

Recommended Action No action is required.

Severity INFO

FCR-1041

Message `<timestamp>, [FCR-1041], <sequence-number>,, INFO, <system-name>, LSAN zone device removed in the backbone fabric.`

Probable Cause Indicates that a logical storage area network (LSAN) zone device within the backbone fabric was removed.

Recommended Action No action is required.

Severity INFO

FCR-1042

Message `<timestamp>, [FCR-1042], <sequence-number>,, INFO, <system-name>, LSAN zone removed in the backbone fabric.`

Probable Cause Indicates that a logical storage area network (LSAN) zone within the backbone fabric was removed.

Recommended Action No action is required.

Severity INFO

FCR-1043

Message

```
<timestamp>, [FCR-1043], <sequence-number>,, INFO,
<system-name>, Proxy device created in the backbone
fabric.
```

Probable Cause

Indicates that a proxy device was created in the backbone fabric.

Recommended Action

No action is required.

Severity

INFO

FCR-1048

Message

```
<timestamp>, [FCR-1048], <sequence-number>,, ERROR,
<system-name>, On EX port (<port number>) setting port
<credit type> credits failed.
```

Probable Cause

Indicates that the specified *credit type* was not set.

Recommended Action

Setting port credits failed. Execute the **portEnable** command.

If the problem persists try rebooting the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

FCR-1049

Message

```
<timestamp>, [FCR-1049], <sequence-number>,, ERROR,
<system-name>, EX port (<port number>) received an ELP
command that is not supported.
```

Probable Cause

Indicates an incoming exchange link protocol (ELP) command was issued and it is not supported.

Recommended Action

Run the **portEnable** and **portDisable** commands to enable and disable the port.

If the problem persists contact the EMC Customer Support Center.

Severity ERROR

FCR-1053

Message `<timestamp>, [FCR-1053], <sequence-number>,, WARNING, <system-name>, Port <port number> was disabled, <disable reason>.`

Probable Cause Indicates that the specified port was disabled because of a mismatched configuration parameter.

Recommended Action Use the specified *disable reason* to identify a possible configuration parameter mismatch between the EX_Port and the switch at other end of the link.

Severity WARNING

FCR-1054

Message `<timestamp>, [FCR-1054], <sequence-number>,, WARNING, <system-name>, Port <port number> received ILS <command> of incorrect size (<actual payload size>); valid ILS size is <expected payload size>.`

Probable Cause Indicates that an internal link service (ILS) IU of invalid size was received from the switch on the other end of the link.

Recommended Action Check the error message log on the other switch using the **errShow** command for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting port.

Run the **fabStateShow** command on transmitting switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FCR-1055

Message

```
<timestamp>, [FCR-1055], <sequence-number>,, INFO,
<system-name>, Switch with domain ID <domain ID> does
not support backbone to edge imports.
```

Probable Cause

Indicates that a switch that does not support backbone-to-edge routing was detected in the backbone. Edge-to-edge routing will work, but backbone-to-edge routing might fail.

Recommended Action

No action is required if backbone to edge routing is not required. Otherwise replace the switch with one that supports backbone to edge routing.

Severity

INFO

FCR-1056

Message

```
<timestamp>, [FCR-1056], <sequence-number>,, INFO,
<system-name>, Switch <switch WWN> with front domain ID
<domain ID> does not support backbone to edge imports.
```

Probable Cause

Indicates that a switch that does not support backbone-to-edge routing is running in the MetaSAN.

Recommended Action

No action is required if backbone-to-edge routing is not needed. Otherwise replace the switch with one that supports backbone to edge routing.

Severity

INFO

FCR-1057

Message

```
<timestamp>, [FCR-1057], <sequence-number>,, ERROR,
<system-name>, EX_Port(<port number>) incompatible long
distance parameters on link.
```

Probable Cause

Indicates that the port, which is configured in long distance mode, has incompatible long distance parameters.

Recommended Action

Check the port configuration on both sides of the link using the **portCfgShow** command.

Investigate the other switch for more details. Run the **errShow** command on the other switch to view the error log for additional messages.

Severity ERROR

FCR-1058

Message

```
<timestamp>, [FCR-1058], <sequence-number>,, WARNING,
<system-name>, Port <port number> isolated due to
mismatched configuration parameter; <segmentation
reason>.
```

Probable Cause Indicates that the specified port was isolated after segmentation, which was caused by mismatched configuration parameters or by a domain ID assigned by the principal switch that did not match the insistent domain ID of this port.

Recommended Action Check the switches on both ends of the link for a possible mismatch in switch or port configuration parameters such as Operating Mode, E_D_TOV, R_A_TOV, Domain ID Offset, etc.

Run the **portCfgExport** command to modify the appropriate parameters on the local switch.

Run the appropriate configuration command to modify the switch or port parameters on the remote switch.

Severity WARNING

FCR-1059

Message

```
<timestamp>, [FCR-1059], <sequence-number>,, INFO,
<system-name>, EX_Port <port number> was disabled due to
an authentication failure.
```

Probable Cause Indicates that the authentication, which uses the Diffie Hellman - challenge handshake authentication Protocol (DH-CHAP), failed on the EX_Port.

Recommended Action Verify that the shared secrets on both sides of the link match.

Disable and enable the ports by using the **portDisable** and the **portEnable** commands to restart authentication.

Severity INFO

FCR-1060

Message `<timestamp>, [FCR-1060], <sequence-number>,, WARNING, <system-name>, EX_Port(<port number>) has an incompatible configuration setting.`

Probable Cause Indicates that virtual channel (VC) Link Init is enabled on the local switch and the remote switch is negotiating in R_RDY mode. The fabric might not form properly.

Recommended Action Check the configuration on the local switch using the **portCfgShow** command to verify that the VC Link Init is disabled, if the remote switch is configured in R_RDY mode or only capable of R_RDY mode.

VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.

R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.

Severity WARNING

FCR-1061

Message `<timestamp>, [FCR-1061], <sequence-number>,, INFO, <system-name>, Backbone fabric created on port <port number>.`

Probable Cause Indicates that a backbone fabric was built on the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1062

Message

```
<timestamp>, [FCR-1062], <sequence-number>,, INFO,
<system-name>, Port <port number> disabled, system only
supports <maximum ports> EX/VEX_ports.
```

Probable Cause Indicates that the maximum number of supported EX_Ports or VEX_Ports was exceeded. To enable the specified port, disable any other operational port then re-enable the port.

Recommended Action No action is required.

Severity INFO

FCR-1063

Message

```
<timestamp>, [FCR-1063], <sequence-number>,, INFO,
<system-name>, Fabric <fabric ID> for switch with domain
ID: <domain ID> mismatch with local fabric ID <local
fabric ID>.
```

Probable Cause Indicates that the fabric ID of the switch does not match the local switch.

Recommended Action Run the **switchShow** command to display the fabric ID. Change the fabric ID to match on both ends by modifying either the local or remote host using the **fcrConfigure** command.

Severity INFO

FCR-1064

Message

```
<timestamp>, [FCR-1064], <sequence-number>,, ERROR,
<system-name>, Fabric ID of backbone FC-Routers mismatch
or overlap.
```

Probable Cause Indicates that either (1) a backbone fabric split and both are connected to common edge fabrics, or (2) the fabric IDs of two backbone fabrics connected to an edge fabric are the same.

Recommended Action If the backbone fabric split, merge the fabrics.

If two (or more) backbone fabrics have the same IDs, make the fabric IDs unique using **fcrConfigure** command.

Severity ERROR

FCR-1065

Message `<timestamp>, [FCR-1065], <sequence-number>,, ERROR, <system-name>, Fabric on port <port number> was assigned two different fabric IDs.`

Probable Cause Indicates that another port on the switch is connected to the same edge fabric with a different fabric ID assignment.

Recommended Action Change the port fabric ID to same value as the other ports connected to the edge fabric using the **portCfgExport** or **portCfgVexport** commands.

Severity ERROR

FCR-1066

Message `<timestamp>, [FCR-1066], <sequence-number>,, ERROR, <system-name>, Fabric on port <port number> has the same fabric ID as another fabric.`

Probable Cause Indicates that either the fabric split, or there is another fabric (possibly the backbone) that has the same fabric ID as the fabric connected to the specified port.

Recommended Action If the fabric split, then merge the fabrics and manually re-enable the port.

If there is another fabric with the same ID, change the fabric ID for the port using the **portCfgExport** or **portCfgVExport** commands.

Severity ERROR

FCR-1067

Message

```
<timestamp>, [FCR-1067], <sequence-number>,, WARNING,
<system-name>, Zone configurations, total LSAN zones and
aliases, exceeded on port <port number> by <overflow>
entries; max entries: <LSAN zone limit>.
```

Probable Cause

Indicates that the total number of zone configurations created in the connected fabric exceeds the maximum number supported by the Fibre Channel router.

The limit includes both active and configured information that is part of the zoning database in the edge fabric. Non-LSAN zones are not counted in the limit.

Recommended Action

Limit the logical storage area network (LSAN) zoning related zone configuration in the edge fabric connected to this port.

Severity

WARNING

FCR-1068

Message

```
<timestamp>, [FCR-1068], <sequence-number>,, INFO,
<system-name>, The FC Routing service is disabled.
```

Probable Cause

Indicates that the FC Routing service is disabled. This is caused by **fosConfig ––disable fcr, configDefault**, or a **configDownload** with the **fcrState** set to 2 (disabled). Note that the FC Routing service is disabled by the factory.

Recommended Action

No action is required.

Severity

INFO

FCR-1069

Message

```
<timestamp>, [FCR-1069], <sequence-number>,, INFO,
<system-name>, The FC Routing service is enabled.
```

Probable Cause

Indicates that the FC Routing service is enabled. This is caused by either **fosConfig –-enable fcr,** or a **configDownload** with the **fcrState**

set to **1** (enabled). Note that the FC Routing service is disabled by the factory.

Recommended Action No action is required.

Severity INFO

FCR-1070

Message `<timestamp>, [FCR-1070], <sequence-number>,, INFO, <system-name>, The FC Routing configuration is set to default.`

Probable Cause Indicates that the FC Routing configuration is set to default by user. This removes all prior FC Routing configurations.

Recommended Action No action is required.

Severity INFO

FCR-1071

Message `<timestamp>, [FCR-1071], <sequence-number>,, INFO, <system-name>, Port <port number> is changed from non FCR port to FCR port.`

Probable Cause Indicates that the port became an EX_Port or VEX_Port.

Recommended Action No action is required.

Severity INFO

FCR-1072

Message `<timestamp>, [FCR-1072], <sequence-number>,, INFO, <system-name>, Port <port number> is changed from FCR port to non FCR port.`

Probable Cause Indicates that the port is no longer an EX_Port or VEX_Port.

Recommended Action No action is required.

Severity INFO

FCR-1073

Message

```
<timestamp>, [FCR-1073], <sequence-number>,, INFO,
<system-name>, Switch with domain ID <domain ID> in
fabric <fabric ID> has lower limit of LSAN Zones
supported.
```

Probable Cause Indicates that a switch in the backbone/edge that supports different limit of logical storage area network (LSAN) zones was detected.

Recommended Action Use the **fcrResourceShow** command on all Fibre Channel Routers in the Meta-SAN to find the lowest supported LSAN zone limits. Make sure that total number of LSAN zones in the Meta-SAN are within the lowest supported limit of LSAN zone.

Severity INFO

FCR-1074

Message

```
<timestamp>, [FCR-1074], <sequence-number>,, ERROR,
<system-name>, HA sync lost as remote CP supports only
<LSAN count> LSAN Zones.
```

Probable Cause Indicates that the remote control processor (CP) has older firmware, which only supports a lower number of logical storage area network (LSAN) zones. This is causing the loss of the high-availability (HA) sync.

Recommended Action Keep the number of LSAN Zones to the lower limit of the two CPs or upgrade the remote CP.

Severity ERROR

FCR-1075

Message

```
<timestamp>, [FCR-1075], <sequence-number>,, ERROR,
<system-name>, Zone Name configuration is larger than
<Zone Name Limit> characters in the edge fabric connected
to port <port numer>.
```

Probable Cause

Indicates that the zone name configuration size created in the connected fabric exceeds the maximum supported by the FC Router. This size is equal to the total number of characters used by all the zone names in the edge fabric zoning database.

The limit includes both logical storage area network (LSAN) and Non-LSAN zone names defined in zoning name database of the edge fabric.

Recommended Action

Limit the zone configuration size in the edge fabric connected to this port by either reducing number of zones or changing the zone names to smaller names.

Severity

ERROR

FCR-1076

Message

```
<timestamp>, [FCR-1076], <sequence-number>,, ERROR,
<system-name>, Port <port number> disabled, system only
supports <maximum fds> front domains.
```

Probable Cause

Indicates that the maximum number of supported front domains was exceeded. To enable the specified port, disable any other operational front domain and then re-enable the port.

Recommended Action

Make sure to remain within the maximum of supported front domains.

Severity

ERROR

FCR-1077

Message

```
<timestamp>, [FCR-1077], <sequence-number>,, WARNING,
<system-name>, Port <port number> rejected fabric binding
request/check from the M-Model switch; <port number>.
```

Probable Cause Indicates that an M-Model edge switch attempted to either activate or check the fabric binding. This port will be disabled if this event occurred during a check of fabric binding and not during failure to activate fabric binding. The error is caused when the binding list details configured on the M-Model switch does not match with the currently configured front port domain ID and WWN of the EX_Port on which this operation was attempted.

Recommended Action Ensure that the M-Model switch has the same currently configured details such as front port domain ID and WWN of the EX_Port on which this operation was attempted.

Severity WARNING

FCR-1078

Message

```
<timestamp>, [FCR-1078], <sequence-number>,, WARNING,
<system-name>, LSAN name <LSAN name> is too long. It is
dropped.
```

Probable Cause The length of the LSAN name exceeds the limit of 64 characters.

Recommended Action Change the name and reactivate the zone database.

Severity WARNING

FCR-1079

Message

```
<timestamp>, [FCR-1079], <sequence-number>,, WARNING,
<system-name>, Domain <Domain> has conflict matrix
database with local domain.
```

Probable Cause The indicated domain has a different LSAN matrix database from the local domain.

Recommended Action Use the **fcrLsanMatrix** command to resolve the matrix differences.

Severity WARNING

FCR-1080

Message

```
<timestamp>, [FCR-1080], <sequence-number>,, WARNING,
<system-name>, The pause response timer for domain
<Domain> expired.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric has not responded to the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

Recommended Action

No action is required.

Severity

WARNING

FCR-1081

Message

```
<timestamp>, [FCR-1081], <sequence-number>,, WARNING,
<system-name>, The pause message is rejected by the
domain <Domain>.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

Recommended Action

No action is required.

Severity

WARNING

FCR-1082

Message

```
<timestamp>, [FCR-1082], <sequence-number>,, WARNING,
<system-name>, The pause retry count is exhausted for the
domain <Domain>.
```

Probable Cause

During the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from

completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

Severity WARNING

FCR-1083

Message `<timestamp>, [FCR-1083], <sequence-number>,, WARNING, <system-name>, The resume message is rejected by the domain <Domain>.`

Probable Cause During the Coordinated HotCode protocol, a switch in the fabric has rejected the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected resume message.

Recommended Action No action is required.

Severity WARNING

FCR-1084

Message `<timestamp>, [FCR-1084], <sequence-number>,, WARNING, <system-name>, The resume retry count is exhausted for the domain <Domain>.`

Probable Cause During the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

Severity WARNING

FCR-1085

Message

```
<timestamp>, [FCR-1085], <sequence-number>,, ERROR,
<system-name>, HA sync lost as remote CP does not support
FCR based matrix.
```

Probable Cause

Indicates that the remote control processor (CP) has an older firmware version which does not support FCR- based matrix, while the local CP has the feature enabled. This is causing the loss of the high-availability (HA) synchronization.

Recommended Action

Run the **firmwareDownload** command to upgrade the firmware on the remote CP to a version that supports FCR.

Severity

ERROR

FCR-1086

Message

```
<timestamp>, [FCR-1086], <sequence-number>,, ERROR,
<system-name>, HA sync lost as remote CP does not support
Condor2 based EX_ports.
```

Probable Cause

Indicates that the remote control processor (CP) has an older firmware version which does not support embedded FCR EX_Port(s). This is causing the loss of the high-availability (HA) synchronization.

Recommended Action

Run the **firmwareDownload** command to upgrade the remote CP to a version that supports embedded FCR, or disable the EX_Port(s).

Severity

ERROR

FCR-1087

Message

```
<timestamp>, [FCR-1087], <sequence-number>,, ERROR,
<system-name>, ExPort <ExPort> connects to fabric
<fabric> with capability to use XISL domain <domain>.
```

Probable Cause

Indicates that the EX_Port connects to a logical fabric containing a domain that has the capability to use XISL.

Recommended Action

Disable the **Allow to use XISL** mode of the domain by using the **configure** command.

Severity ERROR

FCR-1088

Message `<timestamp>, [FCR-1088], <sequence-number>,, INFO, <system-name>, LSAN <Enforce/Speed> tag <Tag Name> added.`

Probable Cause Indicates that an LSAN tag has been added.

Recommended Action No action is required.

Severity INFO

FCR-1089

Message `<timestamp>, [FCR-1089], <sequence-number>,, INFO, <system-name>, LSAN <Enforce/Speed> tag <Tag Name> removed.`

Probable Cause Indicates that an LSAN tag has been removed.

Recommended Action No action is required.

Severity INFO

27

FICN System Messages

This chapter contains information on the following FICON messages.

- FICN-1003 297
- FICN-1004 297
- FICN-1005 297
- FICN-1006 298
- FICN-1007 298
- FICN-1008 298
- FICN-1009 299
- FICN-1010 299
- FICN-1011 300
- FICN-1012 300
- FICN-1013 300
- FICN-1014 301
- FICN-1015 301
- FICN-1016 301
- FICN-1017 302
- FICN-1018 302
- FICN-1019 302
- FICN-1020 303
- FICN-1021 303
- FICN-1022 304
- FICN-1023 304
- FICN-1024 304
- FICN-1025 305
- FICN-1026 305
- FICN-1027 305
- FICN-1028 306
- FICN-1029 306

- FICN-1030 307
- FICN-1031 307
- FICN-1032 307
- FICN-1033 308
- FICN-1034 308
- FICN-1035 308
- FICN-1036 309
- FICN-1037 309
- FICN-1038 309
- FICN-1039 310
- FICN-1040 310
- FICN-1041 310
- FICN-1042 311
- FICN-1043 311
- FICN-1044 312
- FICN-1045 312
- FICN-1046 312
- FICN-1047 313
- FICN-1048 313
- FICN-1049 313
- FICN-1050 314
- FICN-1051 314
- FICN-1052 314
- FICN-1053 315
- FICN-1054 315
- FICN-1055 315
- FICN-1056 316
- FICN-1057 316
- FICN-1058 316
- FICN-1059 317
- FICN-1060 317
- FICN-1061 317
- FICN-1062 318
- FICN-1063 318
- FICN-1064 319
- FICN-1065 319
- FICN-1066 319
- FICN-1067 320
- FICN-1068 320
- FICN-1069 320
- FICN-1070 321
- FICN-1071 321
- FICN-1072 321

- FICN-1073 322
- FICN-1074 322
- FICN-1075 323
- FICN-1076 323
- FICN-1077 324
- FICN-1078 324
- FICN-1079 325
- FICN-1080 325
- FICN-1081 326
- FICN-1082 326
- FICN-1083 326
- FICN-1084 327
- FICN-1085 327
- FICN-1086 327

The FICON messages in this chapter include **<FICON Path>** in many of the messages. The FICON Path is a string that includes, **VEHDHPDDDPLPCUDV** where:

- VE - VE Port Number: This number represents the FCIP Tunnel number through its VE Port number.
- HD - Host switch Domain number: This is a 1 byte hexidecimal value that represents the domain of the switch that the FICON Channel is directly connected to.
- HP - Host Port number: This is a 1 byte hexidecimal value that represents the switch port of the switch that the FICON Channel is directly connected to.
- DD - Device Domain number: This is a 1 byte hexidecimal value that represents the domain of the switch that the FICON Control Unit is directly connected to.
- DP - Device Port number: This is a 1 byte hexidecimal value that represents the switch port of the switch that the FICON Control Unit is directly connected to.
- LP - Host LPAR number: This is a 1 byte hexidecimal value that represents the Logical Partition or Logical Channel Number used on the FICON connection.
- CU - CU Number: This is a 1 byte hexidecimal value that is the Logical Control Unit number (AKA CUADDR) - normally a value in the range of 00-0x1F.

- DV - Device Number: This is a 1 byte hexidecimal value that is the Logical Control Unit number (AKA CUADDR) - normally a value in the range of 00-0xFF

Note that there are some messages where the lower order FICON Path components can be displayed as "**" in those cases, the event or message applicability is not limited to a Device Number or Control Unit or LPAR. Those messages would include the following format of the FICON Path:

- VEHDHPDDDPLPCU** - indicates that the event or message is specific to all Devices on a specific Control Unit.
- VEHDHPDDDPLP**** - indicates that the event or message is specific to all Control Units and all Devices on those control Units from a specific LPAR.
- VEHDHPDDDP****** - indicates that the event or message is specific to all Control Units and all Devices on those control Units from a all LPARs on that FICON Channel.

FICN-1003

Message `<timestamp>, [FICN-1003], <sequence-number>,, WARNING, <system-name>, FICON Tape Emulation License Key is not installed.`

Probable Cause FICON Tape Emulation requires a License Key.

Recommended Action Use the appropriate License Key.

Severity WARNING

FICN-1004

Message `<timestamp>, [FICN-1004], <sequence-number>,, WARNING, <system-name>, FICON XRC Emulation License Key is not installed.`

Probable Cause FICON XRC Emulation requires a License Key.

Recommended Action Use the appropriate License Key.

Severity WARNING

FICN-1005

Message `<timestamp>, [FICN-1005], <sequence-number>,, INFO, <system-name>, FICON GEPort <GE port number> TID <tunnel number> Feature Change verified Xrc <1 or 0 - XRC Emulation Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled> TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 - FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read Block ID Emulation Enabled or Disabled>.`

Probable Cause User changed the configuration manually.

Recommended Action No action is required.

Severity INFO

FICN-1006

Message `<timestamp>, [FICN-1006], <sequence-number>,, WARNING, <system-name>, FICON GEPort < 0 or 1 - GE port number> TID <Tunnel Number> Feature Change failed Xrc <1 or 0 - FICON XRC Emulation Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled> TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 - FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read Block ID Emulation Enabled or Disabled>.`

Probable Cause The FCIP Tunnel ID associated with the FICON tunnel must be down or disabled for a feature change to become effective.

Recommended Action Disable the applicable FCIP tunnel to make the feature change effective.

Severity WARNING

FICN-1007

Message `<timestamp>, [FICN-1007], <sequence-number>,, ERROR, <system-name>, DevDiskEgr:FICON Selective Reset:Path=<FICON PATH> State=0x<current FICON Emulation State> stat_array=0x<last 4 FICON Emulation states>.`

Probable Cause A Selective Reset from the channel was received as either a normal part of path recovery or the starting sequence in an error case.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support.

Severity ERROR

FICN-1008

Message `<timestamp>, [FICN-1008], <sequence-number>,, ERROR, <system-name>, DevDiskEgr:FICON Purge Path received Path=<FICON PATH>.`

Probable Cause FICON Purge Path was received from the channel as a part of path recovery.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1009

Message

```
<timestamp>, [FICN-1009], <sequence-number>,, INFO,
<system-name>, DevIng:CmdReject Sense Data
rcvd:Path=<FICON PATH> LastCmds=0x<last four FICON CCW
Commands processed> Sense Data:Bytes0-0xB=0x<FICON device
Sense Data bytes 0-11>.
```

Probable Cause Unit Check status was received from device and a sense command was issued to read the sense data.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1010

Message

```
<timestamp>, [FICN-1010], <sequence-number>,, INFO,
<system-name>, DevDiskEgr:Device level exception flag
found for Path=<FICON PATH>: Oxid=0x<FC OXID value from
the received Device Level Exception frame>.
```

Probable Cause A Device Level Exception frame was received from the FICON Channel.

Recommended Action If there was a job or IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1011

Message

```
<timestamp>, [FICN-1011], <sequence-number>,, ERROR,
<system-name>, DevDiskIng:XRC Incorrect RRS SeqNum Rcvd
Path=<FICON PATH> Expected=0x<expected RRS sequence
number> Received=0x<received RRS Sequence Number>
Oxid=0x<FC Frame OXID>.
```

Probable Cause

The Control Unit/device presented a Read Record Set Sequence number different from the SDM's expected sequence number.

Recommended Action

If there was an XRC volume or session suspended associated with this event, please contact your vendor's customer support for assistance.

Severity

ERROR

FICN-1012

Message

```
<timestamp>, [FICN-1012], <sequence-number>,, ERROR,
<system-name>, DevDiskIng:Device level exception found
for Path=<FICON PATH>: Oxid=0x<The OXID reported in the
Device Level Exception Frame>.
```

Probable Cause

A Device Level Exception frame was received from the FICON DASD Control Unit.

Recommended Action

If there was a job or IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity

ERROR

FICN-1013

Message

```
<timestamp>, [FICN-1013], <sequence-number>,, INFO,
<system-name>, DevDiskIng:Status=0x<Status that was
received from the DASD device in an odd state> received
in odd state=0x<The current emulation state> from
Path=<FICON PATH> sent LBY.
```

Probable Cause

When the device sent the status in an incorrect state, the Emulation processing rejected the status with a LBY frame.

Recommended Action If there was a job or IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1014

Message `<timestamp>, [FICN-1014], <sequence-number>,, INFO, <system-name>, DevEgr:Device level exception flag found for Path=<FICON PATH>: Oxid=0x<The OXID used to deliver the non-AS Device Level Exception>.`

Probable Cause A frame was received that indicated a device level exception.

Recommended Action If there was an IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1015

Message `<timestamp>, [FICN-1015], <sequence-number>,, ERROR, <system-name>, DevEgr:cuPath=<FICON PATH>:Discarding Invalid LRCd SOF=0x<the received frame SOF type> count=<the running total number of discarded invalid LRC frames>.`

Probable Cause A frame was received from the peer emulation processing with an invalid LRC. This indicates data corruption between the emulation processing components.

Recommended Action Please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1016

Message `<timestamp>, [FICN-1016], <sequence-number>,, INFO, <system-name>, DevIng:Received Logical Path Removed response:Path=<FICON PATH>.`

Probable Cause The FICON Control Unit sent an LPR frame to the FICON channel.

Recommended Action This is an informational message and does not require any action.

Severity INFO

FICN-1017

Message `<timestamp>, [FICN-1017], <sequence-number>,, INFO, <system-name>, DevIng:Received Logical Path Established response:Path=<FICON PATH>.`

Probable Cause The FICON Control Unit sent an LPE frame to the FICON channel.

Recommended Action This is an informational message and does not require any action.

Severity INFO

FICN-1018

Message `<timestamp>, [FICN-1018], <sequence-number>,, ERROR, <system-name>, DevIng:FCUB Lookup failed for Path=<FICON PATH>.`

Probable Cause The FICON Control Unit sent a frame that cannot be associated with a FICON Control Unit CUADDR.

Recommended Action Please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1019

Message `<timestamp>, [FICN-1019], <sequence-number>,, ERROR, <system-name>, DevTapeEgr:AS Link Level Reject (LRJ) from Chan on Path=<FICON PATH> LastCmd=0x<the Last 4 commands issued to the device> LastStatus=0x<the Last 4 status values received from the device>.`

Probable Cause The FICON channel indicated in the path issued an LRJ frame for a sequence from the device.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1020

Message

```
<timestamp>, [FICN-1020], <sequence-number>,, ERROR,
<system-name>, DevTapeEgr:FICON Cancel received
Path=<FICON PATH> state=0x<the current emulation state
for the device> tflags=0x<the current emulation tape
control flags for the device> sflags=0x<the current
emulation status control flags for the device>.
```

Probable Cause The FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1021

Message

```
<timestamp>, [FICN-1021], <sequence-number>,, ERROR,
<system-name>, DevTapeEgr:FICON Tape Cancel:Path=<FICON
PATH> Elapsed Time=<the current SIO time in seconds for
the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Probable Cause The FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1022

Message

```
<timestamp>, [FICN-1022], <sequence-number>,, ERROR,
<system-name>, DevTapeEgr:FICON Selective
Reset:Path=<FICON PATH> State=0x<the current state of the
device that received the selective reset>
statArray=0x<the last 4 status values received from the
device> cmdArray=0x<the last 4 commands that were issued
to the device> tflags=0x<the current emulation tape
control flags for the device> sflags=0x<the current
emulation status control flags for the device>.
```

Probable Cause The FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action If there was an unexpected job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1023

Message

```
<timestamp>, [FICN-1023], <sequence-number>,, ERROR,
<system-name>, DevTapeEgr:FICON Selective
Reset:Path=<FICON PATH> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in
milliseconds for the device> seconds.
```

Probable Cause The FICON channel issued a Selective Reset sequence for a device.

Recommended Action If there was an unexpected job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1024

Message

```
<timestamp>, [FICN-1024], <sequence-number>,, ERROR,
<system-name>, DevTapeEgr:FICON Purge received
Path=<FICON PATH>.
```

Probable Cause The FICON channel issued a Purge Path command sequence for a device.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1025

Message

```
<timestamp>, [FICN-1025], <sequence-number>,, ERROR,
<system-name>, DevTapeIng:Auto Sense Data received on
Path=<FICON PATH> Bytes0-0xB=0x<FICON device Sense Data
bytes 0-11>.
```

Probable Cause The FICON tape write pipelining processed sense data from a FICON device.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1026

Message

```
<timestamp>, [FICN-1026], <sequence-number>,, INFO,
<system-name>,
DevTapeIng:UnusualStatus:WriteCancelSelr:Generating
Final Ending Status Path=<FICON PATH>.
```

Probable Cause The FICON tape write pipeline is completing an emulated Selective Reset sequence.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1027

Message

```
<timestamp>, [FICN-1027], <sequence-number>,, ERROR,
<system-name>, DevTapeIng:Device level exception found
for Path=<FICON PATH>: Oxid=0x<The OXID of the frame that
included the Device Level Exception>.
```

Probable Cause An active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1028

Message

```
<timestamp>, [FICN-1028], <sequence-number>,, ERROR,
<system-name>, HostDiskIng:FICON Cancel received
Path=<FICON PATH> state=0x<The current emulation state of
the device>.
```

Probable Cause An active emulation device received a cancel operation from the FICON channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1029

Message

```
<timestamp>, [FICN-1029], <sequence-number>,, ERROR,
<system-name>, HostDiskIng:FICON Selective
Reset:Path=<FICON PATH> state=0x<The current emulation
state of the device> LastCmds=0x<The last 4 commands
received from the channel for this device>
LastStatus=0x<The last 4 status values presented to the
channel for this device>.
```

Probable Cause An active disk emulation device received a Selective Reset from the FICON channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1030

Message

```
<timestamp>, [FICN-1030], <sequence-number>,, ERROR,
<system-name>, HostDiskIng:FICON Purge
received:Path=<FICON PATH>.
```

Probable Cause An active disk emulation device received a FICON Purge Path from the channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1031

Message

```
<timestamp>, [FICN-1031], <sequence-number>,, WARNING,
<system-name>, HostDiskIng:FICON System Reset received on
Path=<FICON PATH>.
```

Probable Cause The FICON channel sent a System Reset to the disk control unit.

Recommended Action No action is required. The MVS system was either set to IPL or performing error recovery.

Severity WARNING

FICN-1032

Message

```
<timestamp>, [FICN-1032], <sequence-number>,, INFO,
<system-name>, HostDiskIng:XRC Read Channel Extender
Capabilities detected on Path: <FICON PATH>.
```

Probable Cause The XRC System Data mover was restarted to discover the capabilities of the channel extension equipment.

Recommended Action No action is required. This is a part of the XRC initialization.

Severity INFO

FICN-1033

Message

```
<timestamp>, [FICN-1033], <sequence-number>,, INFO,
<system-name>, HostEgr:Logical Path Established on
Path=<FICON PATH>.
```

Probable Cause The peer side FICON Control Unit has accepted a logical path establishment command sequence with the FICON channel.

Recommended Action No action is required. This is a part of the FICON path initialization.

Severity INFO

FICN-1034

Message

```
<timestamp>, [FICN-1034], <sequence-number>,, ERROR,
<system-name>, HostEgr:Discarding Invalid LRCd Frame on
Path=<FICON PATH> count=<The total number of frames that
have been received with an invalid LRC>.
```

Probable Cause The channel emulation processing received a frame with an invalid FICON LRC from the peer. This indicates that the channel side noted corruption from the device/CU side processing.

Recommended Action Please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1035

Message

```
<timestamp>, [FICN-1035], <sequence-number>,, WARNING,
<system-name>, HostIng:FICON System Reset received on
Path=<FICON PATH>.
```

Probable Cause A locally connected FICON channel issued a System Reset to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path initialization.

Severity WARNING

FICN-1036

Message `<timestamp>, [FICN-1036], <sequence-number>,, INFO, <system-name>, HostIng:FICON RLP Request on Path=<FICON PATH>.`

Probable Cause A locally connected FICON Channel issued a Remove Logical Path sequence to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path deactivation.

Severity INFO

FICN-1037

Message `<timestamp>, [FICN-1037], <sequence-number>,, INFO, <system-name>, HostIng:FICON ELP Request on Path=<FICON PATH>.`

Probable Cause A locally connected FICON Channel issued an Establish Logical Path sequence to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path activation.

Severity INFO

FICN-1038

Message `<timestamp>, [FICN-1038], <sequence-number>,, ERROR, <system-name>, fcFicIngHost:FDCB Lookup failed for Path=<FICON PATH>.`

Probable Cause A locally connected FICON channel sent a frame that could not be associated with a FICON device.

Recommended Action Please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1039

Message

```
<timestamp>, [FICN-1039], <sequence-number>,, ERROR,
<system-name>, HostIng:FCUB Lookup failed for Path=<FICON
PATH>.
```

Probable Cause

A locally connected FICON channel sent a frame that could not be associated with a FICON Control Unit.

Recommended Action

Please contact your vendor's customer support for assistance.

Severity

ERROR

FICN-1040

Message

```
<timestamp>, [FICN-1040], <sequence-number>,, ERROR,
<system-name>, HostTapeEgr:Tape:CmdReject Sense Data
Rcvd:Path=<FICON PATH> LastCmds=0x<Last 4 commands
received from the channel for this device>
SenseData:Bytes0-0xB=0x<FICON device Sense Data bytes
0-11>.
```

Probable Cause

An active disk emulation device received a FICON Purge Path from the channel.

Recommended Action

If there was an unexpected job failure or IO Error associated with this event, please contact your vendor's customer support for assistance.

Severity

ERROR

FICN-1041

Message

```
<timestamp>, [FICN-1041], <sequence-number>,, ERROR,
<system-name>, HostTapeEgr:AS Link Level Reject (LRJ)
from CU Rx Path=<FICON PATH> LastCmd=0x<Last 4 commands
issued to this device from the channel>
LastStatus=0x<Last 4 status values sent to the channel
from this device>.
```

Probable Cause

An LRJ received from a device indicates that the CU has lost the logical path to the LPAR.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1042

Message

```
<timestamp>, [FICN-1042], <sequence-number>,, WARNING,
<system-name>, HostTapeIng:FICON Cancel received
Path=<FICON PATH> state=0x<the current emulation state
for this device>.
```

Probable Cause A job was cancelled during write pipelining.

Recommended Action If this was an unexpected event (cancel is normally an operator event), please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1043

Message

```
<timestamp>, [FICN-1043], <sequence-number>,, ERROR,
<system-name>, HostTapeIng::FICON Selective
Reset:Path=<FICON PATH> state=0x<the current emulation
state for this device> LastCmds=0x<the last 4 commands
received from the channel for this device>
LastStatus=0x<the last 4 status values presented to the
channel for this device>.
```

Probable Cause Protocol errors in emulation in the CU or network errors can cause Selective Reset.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1044

Message

```
<timestamp>, [FICN-1044], <sequence-number>,, ERROR,
<system-name>, HostTapeIng:FICON Selective
Reset:Path=<FICON PATH> Elapsed Time=<the number of
seconds since the last IO started for this device>.<the
number of milliseconds since the last IO started for this
device> seconds.
```

Probable Cause Protocol errors in emulation in the CU or network errors can cause Selective Reset.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1045

Message

```
<timestamp>, [FICN-1045], <sequence-number>,, WARNING,
<system-name>, HostTapeIng:FICON Purge
received:Path=<FICON PATH>.
```

Probable Cause Purge path received from the locally connected FICON channel. This is performed during the path recovery.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1046

Message

```
<timestamp>, [FICN-1046], <sequence-number>,, WARNING,
<system-name>, HostTapeIng:LRJ received on Path=<FICON
PATH> lastCmds=0x<Last 4 commands received from the
channel for this device> lastStatus=0x<Last 4 status
values presented to the channel for this device> treating
as system reset event.
```

Probable Cause An LRJ from a FICON channel indicates that the channel believes that it no longer has a path established to the CU.

Recommended Action This is normally an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1047

Message `<timestamp>, [FICN-1047], <sequence-number>,, ERROR, <system-name>, fcFicSetEmulation:Path=<FICON PATH> FDCB Not Idle state=0x<Current emulation state of the FICON device> prevState=0x<Previous emulation state of the FICON device> set to state=0x<The new state to which the device is transitioning>.`

Probable Cause This is an internal emulation error and should not be encountered.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1048

Message `<timestamp>, [FICN-1048], <sequence-number>,, WARNING, <system-name>, DevDiskEgr:FICON Cancel received Path=<FICON PATH> state=0x<Current emulation state of the FICON device> sflags=0x<The current emulation status flags>.`

Probable Cause The operator has cancelled a read or write job.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1049

Message `<timestamp>, [FICN-1049], <sequence-number>,, WARNING, <system-name>, ProcessIngTirData:Lost Logical Path for Path=<FICON PATH> Index=<Current processing index in the TIR data from the locally connected channel or control unit>.`

Probable Cause A TIR received from a FICON end point indicates that it no longer has an established path to its peer.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1050

Message

```
<timestamp>, [FICN-1050], <sequence-number>,, WARNING,
<system-name>, ProcessEgrTirData:Lost Logical Path for
Path=<FICON PATH> Index=<Current processing index in the
TIR data from the remotely connected channel or control
unit>.
```

Probable Cause A TIR received from a far side FICON end point indicates that it no longer has an established path to its peer.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1051

Message

```
<timestamp>, [FICN-1051], <sequence-number>,, INFO,
<system-name>, XRC Session Established: SessID=<SDM
Assigned Session ID>, Path=<FICON PATH>.
```

Probable Cause An establish XRC session PSF command has been received to initiate an XRC session with the extended DASD device.

Recommended Action No action is required. This is a part of the XRC session establishment.

Severity INFO

FICN-1052

Message

```
<timestamp>, [FICN-1052], <sequence-number>,, INFO,
<system-name>, XRC Session Terminated: SessID=<SDM
Assigned Session ID>, Path=<FICON PATH>.
```

Probable Cause A terminate XRC session PSF command has been received to break an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1053

Message

```
<timestamp>, [FICN-1053], <sequence-number>,, INFO,
<system-name>, XRC Withdraw From Session: SessID=<SDM
Assigned Session ID>, Path=<FICON PATH>.
```

Probable Cause A withdraw from XRC session PSF command has been received to break an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1054

Message

```
<timestamp>, [FICN-1054], <sequence-number>,, WARNING,
<system-name>, XRC Device Suspended: SessID=<SDM Assigned
Session ID>, Path=<FICON PATH>.
```

Probable Cause A suspend from XRC session PSF command has been received to break an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1055

Message

```
<timestamp>, [FICN-1055], <sequence-number>,, WARNING,
<system-name>, XRC All Devices Suspended: SessID=<SDM
Assigned Session ID>, Path=<FICON PATH>.
```

Probable Cause A suspend all devices from XRC session PSF command has been received to break an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1056

Message

```
<timestamp>, [FICN-1056], <sequence-number>,, ERROR,
<system-name>, FICON Emulation Error Error Code=<The
internal emulation error code value>, Path=<FICON PATH>
LastStates=0x<The 4 oldest emulation states for this
device>.
```

Probable Cause This is an internal coding error within emulation processing.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1057

Message

```
<timestamp>, [FICN-1057], <sequence-number>,, ERROR,
<system-name>, Error return from frame generation
processing for a FICON device: Path=<FICON PATH>.
```

Probable Cause An internal resource shortage caused error such that an emulation frame could not be created and sent to a device.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1058

Message

```
<timestamp>, [FICN-1058], <sequence-number>,, ERROR,
<system-name>, Error return from frame generation
processing for a FICON control unit: Path=<FICON PATH>.
```

Probable Cause An internal resource shortage caused error such that an emulation frame could not be created and sent to a Control Unit.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1059

Message

```
<timestamp>, [FICN-1059], <sequence-number>,, ERROR,
<system-name>, Error return from frame generation for a
FICON Image: Path=<FICON PATH>.
```

Probable Cause An internal resource shortage caused error such that an emulation frame could not be created and sent to an LPAR.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1060

Message

```
<timestamp>, [FICN-1060], <sequence-number>,, ERROR,
<system-name>, Error return from fcFwdPrcEgressFrame:
Path=<FICON PATH>.
```

Probable Cause An internal resource shortage caused error such that an emulation frame could not be created and sent to a device.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1061

Message

```
<timestamp>, [FICN-1061], <sequence-number>,, ERROR,
<system-name>, Error return from
fcFwdRemoveEmulHashEntry: Path=<FICON PATH>.
```

Probable Cause An internal issue has been encountered in the removal of an existing fast path hash table entry.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1062

Message `<timestamp>, [FICN-1062], <sequence-number>,, ERROR, <system-name>, Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=<FICON PATH>:LastStates=0x<emulation state>.`

Probable Cause An abort operation has been received from the local FC interface for an active emulation exchange.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1063

Message `<timestamp>, [FICN-1063], <sequence-number>,, ERROR, <system-name>, Egress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=<FICON PATH>:LastStates=0x<emulation state>.`

Probable Cause An abort operation has been received from the local FC interface for an active emulation exchange.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1064

Message

```
<timestamp>, [FICN-1064], <sequence-number>,, INFO,
<system-name>, Ingress Abort:Oxid=0x<the OXID of the
aborted exchange>:Unknown Path on GEPort=<GEPort Number>
VEPort=<VEPortNumber> from SID=0x<Source Port> to
DID=0x<Destination Domain><Destination Port>.
```

Probable Cause An abort operation has been received from a local FC interface for an exchange.

Recommended Action If there were associated IO errors at the same time as this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1065

Message

```
<timestamp>, [FICN-1065], <sequence-number>,, INFO,
<system-name>, Egress Abort:Oxid=0x<the OXID of the
aborted exchange>:Unknown Path on GEPort=<GEPort Number>
VEPort=<VEPortNumber> from SID=0x<Source Port> to
DID=0x<Destination Domain><Destination Port>.
```

Probable Cause An abort operation has been received from a peer FC interface for an exchange.

Recommended Action If there were associated IO errors at the same time as this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1066

Message

```
<timestamp>, [FICN-1066], <sequence-number>,, WARNING,
<system-name>, MemAllocFailed for GEPort=<GE0 or GE1
Number> VEport=<VEPortNumber> could not create required
structure.
```

Probable Cause An internal resource limit has been encountered such that additional control block memory could not be allocated.

Recommended Action This is an unexpected event, either the maximum number of emulation devices are already in use or there is an internal memory leak, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1067

Message `<timestamp>, [FICN-1067], <sequence-number>,, ERROR, <system-name>, Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for CH=0x<FICON PATH>.`

Probable Cause An abort operation has been received from a local FC interface for an emulation CH exchange.

Recommended Action If there were associated IO errors at the same time as this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1068

Message `<timestamp>, [FICN-1068], <sequence-number>,, ERROR, <system-name>, Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for CU=0x<FICON PATH>.`

Probable Cause An abort operation has been received from a local FC interface for an emulation CU exchange.

Recommended Action If there were associated IO errors at the same time as this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1069

Message `<timestamp>, [FICN-1069], <sequence-number>,, ERROR, <system-name>, Emulation Configuration Error on TunnelId <Tunnel ID>:.`

Probable Cause An error has been noted in the FICON configuration. Please refer to the string for the nature of the configuration issue.

Recommended Action If resolution of the configuration issue cannot be completed, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1070

Message

```
<timestamp>, [FICN-1070], <sequence-number>,, INFO,
<system-name>, DevTapeIngr:Exceptional Status rcvd on
Path=<FICON PATH> state=0x<current emulation state>
status=0x<the exceptional status value>.
```

Probable Cause The normal end of tape status (0x0D or 0x05) is received from the device or error status (including Unit Check 0x02) is received from an active emulation device.

Recommended Action The end of tape is a normal event during pipelining and not the unit check. If there are associated IO error messages with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1071

Message

```
<timestamp>, [FICN-1071], <sequence-number>,, INFO,
<system-name>, HostTapeIngr:Tape Loaded on Path=<FICON
PATH>.
```

Probable Cause Tape IOs are processed from a locally connected LPAR, which indicates that a tape is loaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1072

Message

```
<timestamp>, [FICN-1072], <sequence-number>,, INFO,
<system-name>, DevTapeEgr:Tape Loaded on Path=<FICON
PATH>.
```

Probable Cause Tape IOs are processed from a locally connected LPAR, which indicates that a tape is loaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1073

Message

```
<timestamp>, [FICN-1073], <sequence-number>,, INFO,
<system-name>, HostTapeIngr:Unloaded:Path=<FICON
PATH>:states=0x<4 prior emulation states>:cmds=0x<last 4
commands received from the channel for this
device>:status=0x<last 4 status values sent to the
channel for this device>:flags=0x<tape report bit flags>.
```

Probable Cause A Rewind and Unload IO has been processed from a locally connected LPAR, which indicates that a tape should be unloaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1074

Message

```
<timestamp>, [FICN-1074], <sequence-number>,, INFO,
<system-name>, HostTapeIngr:WriteReport:Path=<FICON
PATH>:Emuls=0x<the number of idle state to non-idle state
transitions while this tape was loaded>:Cmds=0x<the
number of emulated host write commands processed while
this tape was loaded>:Chains=0x<the number of emulated
host chains processed while this tape was
loaded>:MBytes=<the number of emulated write megabytes
processed while this tape was loaded>.
```

Probable Cause A Rewind and Unload IO has been processed from a locally connected LPAR and write pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1075

Message

```
<timestamp>, [FICN-1075], <sequence-number>,, INFO,
<system-name>, HostTapeIngr:ReadBlkReport:Path=<FICON
PATH>:Emuls=0x<the number of idle state to non-idle state
transitions while this tape was loaded>:Cmds=0x<the
number of emulated host read commands processed while
this tape was loaded>:Chains=0x<the number of emulated
host chains processed while this tape was
loaded>:MBytes=<the number of emulated read megabytes
processed while this tape was loaded>.
```

Probable Cause A Rewind and Unload IO has been processed from a locally connected LPAR and Read Block pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1076

Message

```
<timestamp>, [FICN-1076], <sequence-number>,, INFO,
<system-name>, HostTapeIngr:ReadCpReport:Path=<FICON
PATH>:Emuls=0x<the number of idle state to non-idle state
transitions while this tape was loaded>:Cmds=0x<the
number of emulated host read commands processed while
this tape was loaded>:Chains=0x<the number of emulated
host chains processed while this tape was
loaded>:MBytes=<the number of emulated read megabytes
processed while this tape was loaded>.
```

Probable Cause A Rewind and Unload IO has been processed from a locally connected LPAR and Read Channel Program pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1077

Message

```
<timestamp>, [FICN-1077], <sequence-number>,, INFO,
<system-name>, DevTapeEgr:Unloaded:Path=<FICON
PATH>:states=0x<4 prior emulation states>:cmds=0x<last 4
commands received from the channel for this
device>:status=0x<last 4 status values received from the
channel for this device>:flags=0x<tape report bit flags>.
```

Probable Cause

A Rewind and Unload IO has been processed from a remotely connected LPAR, which indicates that a tape should be unloaded on a device.

Recommended Action

No action is required.

Severity

INFO

FICN-1078

Message

```
<timestamp>, [FICN-1078], <sequence-number>,, INFO,
<system-name>, DevTapeEgr:ReadBlkReport:Path=<FICON
PATH>:Emuls=0x<the number of idle state to non-idle state
transitions while this tape was loaded>:Cmds=0x<the
number of emulated host write commands processed while
this tape was loaded>:Chains=0x<the number of emulated
host chains processed while this tape was
loaded>:MBytes=<the number of emulated write megabytes
processed while this tape was loaded>
```

Probable Cause

A Rewind and Unload IO has been processed from a remotely connected LPAR and Read Block pipelining was performed on the currently loaded tape.

Recommended Action

No action is required.

Severity

INFO

FICN-1079

Message

```
<timestamp>, [FICN-1079], <sequence-number>,, INFO,
<system-name>, DevTapeEgr:WriteReport:Path=<FICON
PATH>:Emuls=0x<the number of idle state to non-idle state
transitions while this tape was loaded>:Cmds=0x<the
number of emulated host read commands processed while
this tape was loaded>:Chains=0x<the number of emulated
host chains processed while this tape was
loaded>:MBytes=<the number of emulated read Kilobytes
processed while this tape was loaded>.
```

Probable Cause

A Rewind and Unload IO has been processed from a remotely connected LPAR and write pipelining was performed on the currently loaded tape.

Recommended Action

No action is required.

Severity

INFO

FICN-1080

Message

```
<timestamp>, [FICN-1080], <sequence-number>,, INFO,
<system-name>, DevTapeEgr:ReadCpReport:Path=<FICON
PATH>:Emuls=0x<the number of idle state to non-idle state
transitions while this tape was loaded>:Cmds=0x<the
number of emulated host read commands processed while
this tape was loaded>:Chains=0x<the number of emulated
host chains processed while this tape was
loaded>:MBytes=<the number of emulated read Kilobytes
processed while this tape was loaded>.
```

Probable Cause

A Rewind and Unload IO has been processed from a remotely connected LPAR and Read Channel Program pipelining was performed on the currently loaded tape.

Recommended Action

No action is required.

Severity

INFO

FICN-1081

Message

```
<timestamp>, [FICN-1081], <sequence-number>,, WARNING,
<system-name>, DevTapeIng:LRJ received on Path=<FICON
PATH> lastCmds=0x<Last 4 commands received from the
channel for this device> lastStatus=0x<Last 4 status
values presented to the channel for this device> treating
as system reset event.
```

Probable Cause An LRJ from a FICON channel indicates that the channel does not have a path established to the CU.

Recommended Action This is normally an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1082

Message

```
<timestamp>, [FICN-1082], <sequence-number>,, WARNING,
<system-name>, EmulEls:CSWR_RSCN received on
GEPort=<GEPortNumber> VEPort=<VEPortNumber>
Domain=0x<Domain Port Host> Port=0x<Device Side>.
```

Probable Cause An attached port which had an FICON emulated path established has logged out from the switch.

Recommended Action This may be an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1083

Message

```
<timestamp>, [FICN-1083], <sequence-number>,, WARNING,
<system-name>, EmulEls:SW_RSCN received on
GEPort=<GEPortNumber> VEPort=<VEPortNumber>
Domain=0x<Domain Port Host> Port=0x<Device Side>.
```

Probable Cause An attached port with the established FICON emulated path has logged out from the switch.

Recommended Action This may be an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1084

Message `<timestamp>, [FICN-1084], <sequence-number>,, ERROR, <system-name>, fcFicInit: No DRAM2 memory available, FICON emulation is disabled.`

Probable Cause A faulty DRAM2 was detected and access to its address range is prohibited.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1085

Message `<timestamp>, [FICN-1085], <sequence-number>,, INFO, <system-name>, FICON FCIP Tunnel is Up on GE<Either GE0 or GE1>,tunnel Id=<The configured tunnel ID (0-7)>.`

Probable Cause A FICON FCIP tunnel has been established successfully to the peer switch.

Recommended Action No action is required.

Severity INFO

FICN-1086

Message `<timestamp>, [FICN-1086], <sequence-number>,, ERROR, <system-name>, FICON FCIP Tunnel is Down on GE<Either GE0 or GE1>,tunnel Id=<The configured tunnel ID (0-7)>.`

Probable Cause A FICON FCIP tunnel has been terminated to the peer switch.

Recommended Action If this is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

28

FICU System Messages

This chapter contains information on the following FICU messages:

- FICU-1001 330
- FICU-1002 330
- FICU-1003 330
- FICU-1004 331
- FICU-1005 332
- FICU-1006 332
- FICU-1007 332
- FICU-1008 333
- FICU-1009 333
- FICU-1010 334

FICU-1001

Message

```
<timestamp>, [FICU-1001], <sequence-number>,, ERROR,
<system-name>, <function name>: config<config
Set(key)|Get(key)| Save> failed rc = <error>.
```

Probable cause

Indicates that one of the configuration management functions failed. The *key* variable is part of the Fabric OS configuration database and is for support use only. The *error* variable is an internal error number.

Recommended action

Execute an **haFailover** on the switch if it has redundant control processors (CPs) or reboot the switch. Run the **supportShow** command to check if your flash is full. If the flash is full, run the **supportSave** command to clear the core files.

Severity

ERROR

FICU-1002

Message

```
<timestamp>, [FICU-1002], <sequence-number>,, ERROR,
<system-name>, <function name>: Failed to get RNID from
Management Server: Domain=<domain>, rc=<error>.
```

Probable cause

Indicates that the fibre connectivity control unit port (FICON-CUP) daemon failed to get the switch request node ID (RNID) from the management server due to a Fabric OS problem. The *domain* variable displays the domain ID of the target switch for this request node ID (RNID). The *error* variable is an internal error number.

Recommended action

If this is a bladed switch, execute the **haFailover** command. If the problem persists, or if this is a nonbladed switch, download a new firmware version using the **firmwareDownload** command.

Severity

ERROR

FICU-1003

Message

```
<timestamp>, [FICU-1003], <sequence-number>,, WARNING,
<system-name>, <function name>: <message> FICON-CUP
License Not Installed: (<error>).
```

Probable cause Indicates that the fibre connectivity control unit port (FICON-CUP) license is not installed on the switch.

Recommended action Run the **licenseShow** command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your EMC account representative for a FICON-CUP license. Run the **licenseAdd** command to add the license to your switch.

Severity WARNING

FICU-1004

Message

```
<timestamp>, [FICU-1004], <sequence-number>,, WARNING,
<system-name>, <function name>: Failed to set fabric
manager server (FMS) mode: conflicting PID
Format:<pid_format>, FMS Mode:<mode>.
```

Probable cause Indicates that a process ID (PID) format conflict was encountered. The core PID format is required for fibre connectivity control unit port (FICON-CUP).

The *pid_format* variable displays the PID format currently running on the fabric, and is one of the following:

- 0 is VC-encoded PID format
- 1 is core PID format
- 2 is extended-edge PID format

FMS mode displays whether fibre connectivity (FICON) Management Server mode is enabled; a 0 means this mode is enabled and a 1 means this mode is disabled.

Recommended action For FICON Management Server mode (**fmsMode**) to be enabled, the core PID format must be used in the fabric. Change the PID format to core PID using the **configure** command and reenable fmsmode using the **ficonCupSet** command. Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for information on the core PID mode.

Severity WARNING

FICU-1005

Message `<timestamp>, [FICU-1005], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module>, rc = <error>.`

Probable cause Indicates that the initialization of a module within the fibre connectivity control unit port (FICON-CUP) daemon failed.

Recommended action Use the **firmwareDownload** command to download a new firmware version.

Severity ERROR

FICU-1006

Message `<timestamp>, [FICU-1006], <sequence-number>,, WARNING, <system-name>, Control Device Allegiance Reset (Logical Path: 0x<PID>:0x<channel image ID>)`

Probable cause Indicates that the path with the specified PID and channel image ID lost allegiance to a fibre connectivity control unit port (FICON-CUP) device.

Recommended action Check if the FICON channel corresponding to the PID in the message is functioning correctly.

Severity WARNING

FICU-1007

Message `<timestamp>, [FICU-1007], <sequence-number>,, WARNING, <system-name>, <function name>: Failed to allocate memory while performing <message>.`

Probable cause Indicates that memory resources are low. This might be a transient problem.

Recommended action If the message persists, check the memory usage on the switch, using the **memShow** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FICU-1008

Message

```
<timestamp>, [FICU-1008], <sequence-number>,, WARNING,
<system-name>, FMS mode has been enabled. Port(s):<port
number(s)> have been disabled due to port address
conflict.
```

Probable cause Indicates that the specified port(s) were disabled when fibre connectivity (FICON) Management Server mode (**fmsMode**) was enabled. This is due to port address conflict or port address being reserved for CUP management port.

Recommended action No action is required.

Severity WARNING

FICU-1009

Message

```
<timestamp>, [FICU-1009], <sequence-number>,, WARNING,
<system-name>, FMS Mode enable failed due to insufficient
frame filtering resources on some ports.
```

Probable cause Indicates that the frame filtering resources required to enable fibre connectivity (FICON) Management Server mode (**fmsMode**) were not available on some of the ports.

Recommended action Use the **perfDelFilterMonitor** command to delete the filter-based performance monitors used on all ports to free up the resources.

Severity WARNING

FICU-1010

Message

```
<timestamp>, [FICU-1010], <sequence-number>,, WARNING,
<system-name>, FMS Mode enable failed due to address
conflict with port <port number>.
```

Probable cause

Indicates that the fibre connectivity FICON Management Server mode (**fmsMode**) was not enabled because the specified port has an address conflict with the CUP management port is in use.

Recommended action

Use the **portDisable** command to disable the specified port to avoid the port address conflict.

Severity

WARNING

29

FKLB System Messages

This chapter contains information on the following FKLB message:

- FKLB-1001 336

FKLB-1001

Message

```
<timestamp>, [FKLB-1001], <sequence-number>,, WARNING,
<system-name>, exchange <xid> overlapped, pid=<pid>
```

Probable cause

Indicates that the FC kernel driver has timed out the exchange while the application is still active. When the FC kernel driver reuses the exchange, the application will overlap. This happens on a timed-out exchange; it automatically recovers after the application times the exchange out.

Recommended action

No action is required.

Severity

WARNING

30

FLOD System Messages

This chapter contains information on the following FLOD messages:

- FLOD-1001 338
- FLOD-1003 338
- FLOD-1004 338
- FLOD-1005 339
- FLOD-1006 339

FLOD-1001

Message

```
<timestamp>, [FLOD-1001], <sequence-number>, FFDC,
WARNING, <system-name>, Unknown LSR type: port <port
number>, type <LSR header type>
```

Probable cause Indicates that the link state record (LSR) type is unknown. 1-Unicast and 3-Multicast are the only two LSR header types.

Recommended action No action is required; the record is discarded.

Severity WARNING

FLOD-1003

Message

```
<timestamp>, [FLOD-1003], <sequence-number>,, WARNING,
<system-name>, Link count exceeded in received LSR, value
= <link count number>
```

Probable cause Indicates that the acceptable link count received was exceeded in the link state record (LSR).

Recommended action No action is required; the record is discarded.

Severity WARNING

FLOD-1004

Message

```
<timestamp>, [FLOD-1004], <sequence-number>, FFDC, ERROR,
<system-name>, Excessive LSU length = <LSU length>
```

Probable cause Indicates that the LSU size exceeds what the system can support.

Recommended action Reduce the number of switches in the fabric or reduce the number of redundant ISLs between two switches.

Severity ERROR

FLOD-1005

Message `<timestamp>, [FLOD-1005], <sequence-number>,, WARNING, <system-name>, Invalid received domain ID: <domain number>`

Probable cause Indicates that the received LSR contained an invalid domain number.

Recommended action No action is required; the LSR is discarded.

Severity WARNING

FLOD-1006

Message `<timestamp>, [FLOD-1006], <sequence-number>,, WARNING, <system-name>, Transmitting invalid domain ID: <domain number>`

Probable cause Indicates that the transmit LSR contained an invalid domain number.

Recommended action No action is required; the LSR is discarded.

Severity WARNING

31

FSPF System Messages

This chapter contains information on the following FSPF messages:

- FSPF-1001 342
- FSPF-1002 342
- FSPF-1003 342
- FSPF-1005 343
- FSPF-1006 343

FSPF-1001

Message `<timestamp>, [FSPF-1001], <sequence-number>,, ERROR, <system-name>, Input Port <port number> out of range`

Probable cause Indicates that the specified input port number is out of range; it does not exist on the switch.

Recommended action No action is required.

Severity ERROR

FSPF-1002

Message `<timestamp>, [FSPF-1002], <sequence-number>,, INFO, <system-name>, Wrong neighbor ID (<domain ID>) in Hello message from port <port number>, expected ID = <domain ID>`

Probable cause Indicates that the switch received the wrong domain ID from a neighbor (adjacent) switch in the HELLO message from a specified port. This might happen when a domain ID for a switch has been changed.

Recommended action No action is required.

Severity INFO

FSPF-1003

Message `<timestamp>, [FSPF-1003], <sequence-number>,, ERROR, <system-name>, Remote Domain ID <domain number> out of range, input port = <port number>`

Probable cause Indicates that the specified remote domain ID is out of range.

Recommended action No action is required; the frame is discarded.

Severity ERROR

FSPF-1005

Message

```
<timestamp>, [FSPF-1005], <sequence-number>,, ERROR,
<system-name>, Wrong Section Id <section number>, should
be <section number>, input port = <port number>
```

Probable cause

Indicates that an incorrect section ID was reported from the specified input port. The section ID is used to identify a set of switches that share an identical topology database. The section ID is implemented inside the protocol. The error message itself will indicate the mismatched section ID. It should be set to 0 for a nonhierarchical fabric. EMC switches support only section ID 0.

Recommended action

Use a frame analyzer to verify that the reported section ID is 0. Any connected (other manufacturer) switch with a section ID other than 0 is incompatible in a fabric of Connectrix B switches. Disconnect the offending switch.

Severity

ERROR

FSPF-1006

Message

```
<timestamp>, [FSPF-1006], <sequence-number>,, ERROR,
<system-name>, FSPF Version <FSFP version> not supported,
input port = <port number>
```

Probable cause

Indicates that the FSPF version is not supported on the specified input port.

Recommended action

Update the FSPF version by running the **firmwareDownload** command to update the firmware to the latest version. All current versions of the Fabric OS support FSPF version 2, which is the correct version.

Severity

ERROR

32

FSS System Messages

This chapter contains information on the following FSS messages:

- FSS-1001 346
- FSS-1002 346
- FSS-1003 346
- FSS-1004 347
- FSS-1005 347
- FSS-1006 348
- FSS-1007 348
- FSS-1008 348
- FSS-1009 349
- FSS-1010 349
- FSS-1011 349

FSS-1001

Message

```
<timestamp>, [FSS-1001], <sequence-number>,, WARNING,
<system-name>, Component (<component name>) dropping HA
data update (<update ID>).
```

Probable cause

Indicates that an application has dropped a high availability (HA) data update.

Recommended action

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

FSS-1002

Message

```
<timestamp>, [FSS-1002], <sequence-number>,, WARNING,
<system-name>, Component (<component name>) sending too
many concurrent HA data update transactions (<dropped
update transaction ID>)
```

Probable cause

Indicates that an application has sent too many concurrent high availability (HA) data updates.

Recommended action

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

FSS-1003

Message

```
<timestamp>, [FSS-1003], <sequence-number>,, WARNING,
<system-name>, Component (<component name>) misused the
update transaction (<transaction ID>) without marking the
transaction beginning.
```

Probable cause Indicates that the Fabric OS state synchronization (FSS) service has dropped the update because an application has not set the transaction flag correctly.

Recommended action Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FSS-1004

Message

```
<timestamp>, [FSS-1004], <sequence-number>,, ERROR,
<system-name>, Memory shortage
```

Probable cause Indicates that the system ran out of memory.

Recommended action Run the **memShow** command to view memory usage.

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

FSS-1005

Message

```
<timestamp>, [FSS-1005], <sequence-number>,, WARNING,
<system-name>, FSS read failure
```

Probable cause Indicates that the read system call to the Fabric OS state synchronization (FSS) device failed.

Recommended action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FSS-1006

Message `<timestamp>, [FSS-1006], <sequence-number>,, WARNING, <system-name>, No FSS message available`

Probable cause Indicates that data is not available on the Fabric OS state synchronization (FSS) device.

Recommended action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

FSS-1007

Message `<timestamp>, [FSS-1007], <sequence-number>,, CRITICAL, <system-name>, <component name>: Faulty Ethernet connection.`

Probable cause Indicates that the Ethernet connection between the active control processor (CP) and standby CP is not healthy. The error occurs when the standby CP does not respond to a request from the active CP within 5 seconds. This usually indicates a problem with the internal Ethernet connection and a disruption of the synchronization process.

Recommended action Check the Ethernet connection between active CP and standby CP (interface eth1) by issuing net commands such as **ifconfig eth1** (as root) or run **supportShow**/**supportSave** to validate the network configuration; then try to restore the synchronization by issuing the **haSyncStart** command. If the problem persists, contact the EMC Customer Support Center.

Severity CRITICAL

FSS-1008

Message `<timestamp>, [FSS-1008], <sequence-number>,, CRITICAL, <system-name>, FSS Error: <Error Message>.`

Probable Cause Indicates that a critical error has occurred.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity CRITICAL

FSS-1009

Message `<timestamp>, [FSS-1009], <sequence-number>,, ERROR, <system-name>, FSS Error: <Error Message>.`

Probable Cause Indicates that an error has occurred.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

FSS-1010

Message `<timestamp>, [FSS-1010], <sequence-number>,, WARNING, <system-name>, FSS Warning: <Warning Message>.`

Probable Cause Indicates that an error might have occurred.

Recommended Action No action is required.

Severity WARNING

FSS-1011

Message `<timestamp>, [FSS-1011], <sequence-number>,, INFO, <system-name>, FSS Info: <Info Message>.`

Probable Cause Indicates that an error has occurred.

Recommended Action No action is required.

Severity INFO

33

FSSM System Messages

This chapter contains information on the following FSSM messages:

- FSSM-1002 352
- FSSM-1003 352
- FSSM-1004 352

FSSM-1002

Message

```
<timestamp>, [FSSM-1002], <sequence-number>,, INFO,
<system-name>, HA State is in sync.
```

Probable cause

Indicates that the high availability (HA) state for the active control processor (CP) is in synchronization with the HA state of the standby CP. If the standby CP is healthy, then a failover is nondisruptive.

Recommended action

No action is required.

Severity

INFO

FSSM-1003

Message

```
<timestamp>, [FSSM-1003], <sequence-number>,, WARNING,
<system-name>, HA State out of sync.
```

Probable cause

Indicates that the high availability (HA) state for the active control processor (CP) is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of sync, the failover is disruptive.

Recommended action

If this message was logged as a result of a user-initiated action (such as running the **switchReboot** command), then no action is required.

Otherwise, issue the **haSyncStart** command on the active CP and try resynchronizing the HA state. If the HA state does not become synchronized, run the **haDump** command to diagnose the problem.

If the problem persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

FSSM-1004

Message

```
<timestamp>, [FSSM-1004], <sequence-number>,, INFO,
<system-name>, Incompatible software version in HA
synchronization.
```

Probable cause Indicates that the active control processor (CP) and the standby CP in a dual CP system are running firmware that are incompatible with each other. If the active CP fails, the failover will be disruptive. In a non-bladed system, this message is logged when the firmware upgrade/downgrade was invoked. The new firmware version is not compatible with current running version. This cause a disruptive firmware upgrade/downgrade.

Recommended action For a dual CP system, run the **firmwareDownload** command to load compatible firmware on the standby CP.

Severity INFO

34

FW System Messages

This chapter contains information on the following FW messages:

- FW-1001 361
- FW-1002 361
- FW-1003 362
- FW-1004 362
- FW-1005 362
- FW-1006 363
- FW-1007 363
- FW-1008 364
- FW-1009 364
- FW-1010 364
- FW-1011 365
- FW-1012 365
- FW-1033 366
- FW-1034 366
- FW-1035 366
- FW-1036 367
- FW-1037 367
- FW-1038 368
- FW-1039 368
- FW-1040 368
- FW-1041 369
- FW-1042 369
- FW-1043 370
- FW-1044 370
- FW-1045 371
- FW-1046 371
- FW-1047 371

- FW-1048 372
- FW-1049 372
- FW-1050 373
- FW-1051 373
- FW-1052 373
- FW-1113 374
- FW-1114 374
- FW-1115 375
- FW-1116 375
- FW-1117 376
- FW-1118 376
- FW-1119 377
- FW-1120 377
- FW-1121 378
- FW-1122 378
- FW-1123 379
- FW-1124 379
- FW-1125 379
- FW-1126 380
- FW-1127 381
- FW-1128 381
- FW-1129 382
- FW-1130 382
- FW-1131 382
- FW-1132 383
- FW-1133 383
- FW-1134 384
- FW-1135 384
- FW-1136 384
- FW-1137 385
- FW-1138 385
- FW-1139 386
- FW-1140 386
- FW-1160 386
- FW-1161 387
- FW-1162 387
- FW-1163 388
- FW-1164 388
- FW-1165 389
- FW-1166 389
- FW-1167 390
- FW-1168 390
- FW-1169 391

- FW-1170 391
- FW-1171 391
- FW-1172 392
- FW-1173 392
- FW-1174 393
- FW-1175 393
- FW-1176 394
- FW-1177 394
- FW-1178 394
- FW-1179 395
- FW-1180 395
- FW-1181 396
- FW-1182 396
- FW-1183 396
- FW-1184 397
- FW-1185 397
- FW-1186 398
- FW-1187 398
- FW-1188 398
- FW-1189 399
- FW-1190 399
- FW-1191 399
- FW-1192 400
- FW-1193 400
- FW-1194 401
- FW-1195 401
- FW-1196 401
- FW-1197 402
- FW-1198 402
- FW-1199 403
- FW-1216 403
- FW-1217 404
- FW-1218 404
- FW-1219 405
- FW-1240 405
- FW-1241 406
- FW-1242 406
- FW-1243 407
- FW-1244 407
- FW-1245 408
- FW-1246 408
- FW-1247 408
- FW-1248 409

- FW-1249 409
- FW-1250 410
- FW-1251 410
- FW-1272 410
- FW-1273 411
- FW-1274 411
- FW-1275 412
- FW-1296 412
- FW-1297 413
- FW-1298 413
- FW-1299 414
- FW-1300 414
- FW-1301 415
- FW-1302 415
- FW-1303 416
- FW-1304 416
- FW-1305 417
- FW-1306 417
- FW-1307 418
- FW-1308 418
- FW-1309 419
- FW-1310 419
- FW-1311 419
- FW-1312 420
- FW-1313 420
- FW-1314 421
- FW-1315 421
- FW-1316 422
- FW-1317 422
- FW-1318 423
- FW-1319 423
- FW-1320 424
- FW-1321 424
- FW-1322 425
- FW-1323 425
- FW-1324 426
- FW-1325 426
- FW-1326 426
- FW-1327 427
- FW-1328 427
- FW-1329 428
- FW-1330 428
- FW-1331 429

- FW-1332 429
- FW-1333 430
- FW-1334 430
- FW-1335 431
- FW-1336 431
- FW-1337 432
- FW-1338 432
- FW-1339 433
- FW-1340 433
- FW-1341 434
- FW-1342 434
- FW-1343 434
- FW-1344 435
- FW-1345 435
- FW-1346 436
- FW-1347 436
- FW-1348 437
- FW-1349 437
- FW-1350 438
- FW-1351 438
- FW-1352 439
- FW-1353 440
- FW-1354 440
- FW-1355 441
- FW-1356 441
- FW-1357 442
- FW-1358 442
- FW-1359 443
- FW-1360 443
- FW-1361 444
- FW-1362 444
- FW-1363 444
- FW-1364 445
- FW-1365 445
- FW-1366 446
- FW-1367 446
- FW-1368 446
- FW-1369 447
- FW-1370 447
- FW-1371 448
- FW-1372 448
- FW-1373 449
- FW-1374 449

- FW-1375 450
- FW-1376 450
- FW-1377 451
- FW-1378 451
- FW-1379 452
- FW-1400 452
- FW-1401 453
- FW-1402 453
- FW-1403 454
- FW-1424 454
- FW-1425 454
- FW-1426 455
- FW-1427 455
- FW-1428 455
- FW-1429 456
- FW-1430 456
- FW-1431 456
- FW-1432 457
- FW-1433 457
- FW-1434 458
- FW-1435 458
- FW-1436 458
- FW-1437 459
- FW-1438 459
- FW-1439 460
- FW-1440 460
- FW-1441 460
- FW-1442 461
- FW-1443 461
- FW-1444 461
- FW-1445 462
- FW-1446 462
- FW-1500 463
- FW-1501 463
- FW-1510 463

FW-1001

Message

```
<timestamp>, [FW-1001], <sequence-number>,, INFO,
<system-name>, <label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the internal temperature of the switch has changed.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

Severity

INFO

FW-1002

Message

```
<timestamp>, [FW-1002], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary (High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the internal temperature of the switch has fallen below the low boundary.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures means that the fans and airflow of a switch are functioning normally.

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Severity

WARNING

FW-1003

Message

```
<timestamp>, [FW-1003], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the internal temperature of the switch has risen above the high boundary to a value that might damage the switch.

Recommended action

This message generally appears when a fan fails. If so, a fan-failure message accompanies this message. Replace the fan field-replaceable unit (FRU).

Severity

WARNING

FW-1004

Message

```
<timestamp>, [FW-1004], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

Severity

INFO

FW-1005

Message

```
<timestamp>, [FW-1005], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the speed of the fan has changed. Fan problems typically contribute to temperature problems.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

Severity INFO

FW-1006

Message

```
<timestamp>, [FW-1006], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the speed of the fan has fallen below the low boundary. Fan problems typically contribute to temperature problems.

Recommended action Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan field-replaceable unit (FRU).

Severity WARNING

FW-1007

Message

```
<timestamp>, [FW-1007], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the speed of the fan has risen above the high boundary. Fan problems typically contribute to temperature problems.

Recommended action Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan field-replaceable unit (FRU).

Severity WARNING

FW-1008

Message

```
<timestamp>, [FW-1008], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the speed of the fan has changed from a value outside of the acceptable range to a value within the acceptable range. Fan problems typically contribute to temperature problems.

Recommended action

No action is required. Consistently abnormal fan speeds generally indicate that the fan is failing. If this message occurs repeatedly, replace the fan field-replaceable unit (FRU).

Severity

INFO

FW-1009

Message

```
<timestamp>, [FW-1009], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the state of the power supply has changed from faulty to functional, or from functional to faulty.

Recommended action

If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Run the **psShow** command to view the status of the power supply. If the power supply continues to be a problem, replace the faulty power supply.

Severity

INFO

FW-1010

Message

```
<timestamp>, [FW-1010], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the power supply is faulty. The power supply is not producing enough power.

Recommended action Verify that you have installed the power supply correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

Severity WARNING

FW-1011

Message

```
<timestamp>, [FW-1011], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the power supply is functioning properly.

Recommended action Set the high boundary above the normal operation range.

Severity INFO

FW-1012

Message

```
<timestamp>, [FW-1012], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the power supply counter changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1033

Message

```
<timestamp>, [FW-1033], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the temperature of the small form-factor pluggable (SFP) has changed. Frequent fluctuations in SFP temperature might indicate a deteriorating SFP.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1034

Message

```
<timestamp>, [FW-1034], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the temperature of the small form-factor pluggable (SFP) has fallen below the low boundary.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity WARNING

FW-1035

Message

```
<timestamp>, [FW-1035], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the temperature of the small form-factor pluggable (SFP) has risen above the high boundary. Frequent fluctuations in temperature might indicate a deteriorating SFP.

Recommended action Replace the SFP.

Severity WARNING

FW-1036

Message `<timestamp>, [FW-1036], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable cause Indicates that the temperature of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. Frequent fluctuations in temperature might indicate a deteriorating SFP.

Recommended action No action is required.

Severity INFO

FW-1037

Message `<timestamp>, [FW-1037], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable cause Indicates that the receive power value of the small form-factor pluggable (SFP) has changed. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action Incoming laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

Severity INFO

FW-1038

Message

```
<timestamp>, [FW-1038], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the receive power value of the small form-factor pluggable (SFP) has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity

WARNING

FW-1039

Message

```
<timestamp>, [FW-1039], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the receive power value of the small form-factor pluggable (SFP) has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action

Replace the SFP before it deteriorates.

Severity

WARNING

FW-1040

Message

```
<timestamp>, [FW-1040], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the receive power value of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1041

Message

```
<timestamp>, [FW-1041], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has changed. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action Transmitting laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

Severity INFO

FW-1042

Message

```
<timestamp>, [FW-1042], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity WARNING

FW-1043

Message

```
<timestamp>, [FW-1043], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action Replace the SFP.

Severity WARNING

FW-1044

Message

```
<timestamp>, [FW-1044], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1045

Message

```
<timestamp>, [FW-1045], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the value of the small form-factor pluggable (SFP) voltage has changed. If the supplied voltage of the SFP transceiver is outside of the normal range, this might indicate a hardware failure.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent messages indicate that you must replace the SFP.

Severity

INFO

FW-1046

Message

```
<timestamp>, [FW-1046], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the value of the small form-factor pluggable (SFP) voltage has fallen below the low boundary.

Recommended action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity

WARNING

FW-1047

Message

```
<timestamp>, [FW-1047], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the value of the small form-factor pluggable (SFP) voltage has risen above the high boundary. The supplied current of

the SFP transceiver is outside of the normal range, indicating possible hardware failure.

Recommended action If the current rises above the high boundary, you must replace the SFP.

Severity WARNING

FW-1048

Message

```
<timestamp>, [FW-1048], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1049

Message

```
<timestamp>, [FW-1049], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed. Frequent voltage fluctuations are an indication that the SFP is deteriorating.

Recommended action Replace the SFP if you see frequent voltage fluctuations.

Severity INFO

FW-1050

Message

```
<timestamp>, [FW-1050], <sequence-number>,, WARNING,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the value of the small form-factor pluggable (SFP) voltage has fallen below the low boundary.

Recommended action Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out_of_Range). If continuous or repeated alarms occur, replace the SFP before it deteriorates.

Severity WARNING

FW-1051

Message

```
<timestamp>, [FW-1051], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the value of the small form-factor pluggable (SFP) voltage has risen above the high boundary. High voltages indicate possible hardware failures. Frequent voltage fluctuations are an indication that the SFP is deteriorating.

Recommended action If you see frequent voltage fluctuations, replace the SFP.

Severity WARNING

FW-1052

Message

```
<timestamp>, [FW-1052], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1113

Message

```
<timestamp>, [FW-1113], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of times E_Ports have gone down has changed. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended action Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

Severity INFO

FW-1114

Message

```
<timestamp>, [FW-1114], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of times E_Ports have gone down has fallen below the low boundary. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors. A low number of E_Port failures means that the switch is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1115

Message

```
<timestamp>, [FW-1115], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of times E_Ports have gone down has risen above the high boundary. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Check both ends of the physical connection and verify that the SFP functions properly.

Severity

INFO

FW-1116

Message

```
<timestamp>, [FW-1116], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of times E_Ports have gone down has changed from a value outside of the acceptable range to a value within the acceptable range. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1117

Message

```
<timestamp>, [FW-1117], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of fabric reconfigurations has changed. The following actions can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended action

Verify that the cable is properly connected at both ends. Verify that the small form-factor pluggables (SFPs) have not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

Severity

INFO

FW-1118

Message

```
<timestamp>, [FW-1118], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of fabric reconfigurations has fallen below the low boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

A low number of fabric reconfigurations means that the fabric is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1119

Message

```
<timestamp>, [FW-1119], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of fabric reconfigurations has risen above the high boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended action Verify that all interswitch link (ISL) cables are properly connected at both ends. Verify that the small form-factor pluggable (SFP) has not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

Severity INFO

FW-1120

Message

```
<timestamp>, [FW-1120], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of fabric reconfigurations has changed from a value outside of the acceptable range to a value within the acceptable range. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.

- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1121

Message

```
<timestamp>, [FW-1121], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of domain ID changes has changed. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1122

Message

```
<timestamp>, [FW-1122], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of domain ID changes has fallen below the low boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch. A low number of domain ID changes means that the fabric is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1123

Message

```
<timestamp>, [FW-1123], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of domain ID changes has risen above the high boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1124

Message

```
<timestamp>, [FW-1124], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of domain ID changes has changed from a value outside of the acceptable range to a value within the acceptable range. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1125

Message

```
<timestamp>, [FW-1125], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of segmentations has changed. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1126

Message

```
<timestamp>, [FW-1126], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of segmentations has fallen below the low boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

A low number of segmentation errors means that the fabric is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1127

Message

```
<timestamp>, [FW-1127], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of segmentations has risen above the high boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1128

Message

```
<timestamp>, [FW-1128], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of segmentations has changed from a value outside of the acceptable range to a value within the acceptable range. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1129

Message

```
<timestamp>, [FW-1129], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of zone changes has changed. Zone changes occur when there is a change to the effective zone configuration.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1130

Message

```
<timestamp>, [FW-1130], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of zone changes has fallen below the low boundary. Zone changes occur when there is a change to the effective zone configuration. A low number of zone configuration changes means that the fabric is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1131

Message

```
<timestamp>, [FW-1131], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of zone changes has risen above the high boundary. Zone changes occur when there is a change to the effective zone configuration.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1132

Message

```
<timestamp>, [FW-1132], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of zone changes has changed from a value outside of the acceptable range to a value within the acceptable range. Zone changes occur when there is a change to the effective zone configuration.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1133

Message

```
<timestamp>, [FW-1133], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of fabric logins has changed. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1134

Message

```
<timestamp>, [FW-1134], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of fabric logins has fallen below the low boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI. A low number of fabric logins means that the fabric is functioning normally.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1135

Message

```
<timestamp>, [FW-1135], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of fabric logins has risen above the high boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1136

Message

```
<timestamp>, [FW-1136], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of fabric logins has changed from a value outside of the acceptable range to a value within the acceptable

range. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1137

Message

```
<timestamp>, [FW-1137], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of small form-factor pluggable (SFP) state changes has changed. SFP state changes occur when the SFP is inserted or removed.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1138

Message

```
<timestamp>, [FW-1138], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of small form-factor pluggable (SFP) state changes has fallen below the low boundary. SFP state changes occur when the SFP is inserted or removed. A low number of SFP state changes means that the switch is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1139

Message

```
<timestamp>, [FW-1139], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of small form-factor pluggable (SFP) state changes has risen above the high boundary. SFP state changes occur when the SFP is inserted or removed.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1140

Message

```
<timestamp>, [FW-1140], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of small form-factor pluggable (SFP) state changes has changed from a value outside of the acceptable range to a value within the acceptable range. SFP state changes occur when the SFP is inserted or removed.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1160

Message

```
<timestamp>, [FW-1160], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of link failures that the port experiences has changed. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link

loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Losses of synchronization commonly causes link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

Severity INFO

FW-1161

Message

```
<timestamp>, [FW-1161], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of link failures that the port experiences has fallen below the low boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them. A low number of link loss errors means that the switch is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1162

Message

```
<timestamp>, [FW-1162], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of link failures that the port experiences has risen above the high boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware

problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Losses of synchronization commonly cause link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

Severity WARNING

FW-1163

Message

```
<timestamp>, [FW-1163], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause Indicates that the number of link failures that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1164

Message

```
<timestamp>, [FW-1164], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of synchronization losses that the port experiences has changed. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

If you continue to experience synchronization loss errors, troubleshoot your host bus adaptor (HBA) and contact the EMC Customer Support Center.

Severity

INFO

FW-1165

Message

```
<timestamp>, [FW-1165], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of synchronization losses that the port experiences has fallen below the low boundary. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of synchronization losses means that the switch is functioning normally.

Severity

INFO

FW-1166

Message

```
<timestamp>, [FW-1166], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of synchronization losses that the port experiences has risen above the high boundary.
Loss-of-synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

If you continue to experience loss-of-synchronization errors, troubleshoot your host bus adaptor (HBA) and contact the EMC Customer Support Center.

Severity WARNING

FW-1167

Message

```
<timestamp>, [FW-1167], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause Indicates that the number of synchronization losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1168

Message

```
<timestamp>, [FW-1168], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of signal losses that the port experiences has changed. Loss of signal generally indicates a physical problem.

Recommended action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1169

Message

```
<timestamp>, [FW-1169], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of signal losses that the port experiences has fallen below the low boundary. Loss of signal generally indicates a physical problem.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of signal loss errors means that the switch is functioning normally.

Severity

INFO

FW-1170

Message

```
<timestamp>, [FW-1170], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of signal losses that the port experiences has risen above the high boundary. Loss of signal generally indicates a physical problem.

Recommended action

Check both ends of your cable connection. Verify that the cable is not faulty.

Severity

WARNING

FW-1171

Message

```
<timestamp>, [FW-1171], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause

Indicates that the number of signal losses that the port experiences has changed from a value outside of the acceptable range to a value

within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent loss of signal generally indicates a physical problem.

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1172

Message

```
<timestamp>, [FW-1172], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of protocol errors that the port experiences has changed. Occasional protocol errors occur due to intermittent software errors. Persistent protocol errors occur due to hardware problems.

Recommended action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1173

Message

```
<timestamp>, [FW-1173], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of protocol errors that the port experiences has fallen below the low boundary. Occasional protocol errors occur due to intermittent software errors. Persistent protocol errors occur due to hardware problems. A low number of protocol errors means that the switch is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1174

Message

```
<timestamp>, [FW-1174], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of protocol errors that the port experiences has risen above the high boundary. Occasional protocol errors occur due to intermittent software errors. Persistent protocol errors occur due to hardware problems.

Recommended action Check both ends of your connection. Verify that your cable and small form-factor pluggable (SFP) are not faulty.

Severity WARNING

FW-1175

Message

```
<timestamp>, [FW-1175], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause Indicates that the number of protocol errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Occasional protocol errors occur due to intermittent software errors. Persistent protocol errors occur due to hardware problems.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1176

Message

```
<timestamp>, [FW-1176], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid words that the port experiences has changed. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable.

Recommended action Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

Severity INFO

FW-1177

Message

```
<timestamp>, [FW-1177], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid words that the port experiences has fallen below the low boundary. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable. A low number of invalid words means that the switch is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1178

Message

```
<timestamp>, [FW-1178], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid words that the port experiences has risen above the high boundary. Invalid words usually indicate a

hardware problem with an small form-factor pluggable (SFP) or cable.

Recommended action Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

Severity WARNING

FW-1179

Message

```
<timestamp>, [FW-1179], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid words that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1180

Message

```
<timestamp>, [FW-1180], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity INFO

FW-1181

Message

```
<timestamp>, [FW-1181], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has fallen below the low boundary.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid CRCs means that the switch is functioning normally.

Severity

INFO

FW-1182

Message

```
<timestamp>, [FW-1182], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has risen above the high boundary.

Recommended action

This error generally indicates an deteriorating fabric hardware. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity

WARNING

FW-1183

Message

```
<timestamp>, [FW-1183], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity INFO

FW-1184

Message

```
<timestamp>, [FW-1184], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of incoming traffic that the port experiences has changed.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1185

Message

```
<timestamp>, [FW-1185], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of incoming traffic that the port experiences has fallen below the low boundary.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1186

Message

```
<timestamp>, [FW-1186], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of incoming traffic that the port experiences has risen above the high boundary.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1187

Message

```
<timestamp>, [FW-1187], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of incoming traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1188

Message

```
<timestamp>, [FW-1188], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of outgoing traffic that the port experiences has changed.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1189

Message

```
<timestamp>, [FW-1189], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of outgoing traffic that the port experiences has fallen below the low boundary.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1190

Message

```
<timestamp>, [FW-1190], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of outgoing traffic that the port experiences has risen above the high boundary.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1191

Message

```
<timestamp>, [FW-1191], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause Indicates that the percentage of outgoing traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1192

Message

```
<timestamp>, [FW-1192], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of state changes that the port experiences has changed. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1193

Message

```
<timestamp>, [FW-1193], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of state changes that the port experiences has fallen below the low boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

A low number of port state changes means that the switch is functioning normally.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1194

Message

```
<timestamp>, [FW-1194], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of state changes that the port experiences has risen above the high boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

WARNING

FW-1195

Message

```
<timestamp>, [FW-1195], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable cause

Indicates that the number of state changes that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1196

Message

```
<timestamp>, [FW-1196], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, value has
changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable Cause Indicates that the number of link resets that the port experiences has changed. Link resets occur due to link timeout errors that indicate no frame activity at all.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs.

Severity INFO

FW-1197

Message

```
<timestamp>, [FW-1197], <sequence-number>,, INFO,
<system-name>, <Port Name>, <Label>, is below low
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable Cause Indicates that the number of link resets that the port experiences has fallen below the low boundary. Link resets occur due to link timeout errors that indicate no frame activity at all.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of link resets means that the switch is functioning normally.

Severity INFO

FW-1198

Message

```
<timestamp>, [FW-1198], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is above high
boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable Cause Indicates that the number of link resets that the port experiences has risen above the high boundary. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs.

Severity WARNING

FW-1199

Message

```
<timestamp>, [FW-1199], <sequence-number>,, WARNING,
<system-name>, <Port Name>, <Label>, is between high and
low boundaries (High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the number of link resets that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1216

Message

```
<timestamp>, [FW-1216], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of arbitrated loop physical address (AL_PA) cyclic redundancy check (CRC) errors has changed. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended action

Verify that your optical components are clean and function properly. Replace deteriorating cables or small form-factor pluggables (SFPs). Check for damage from heat or age. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

Severity

INFO

FW-1217

Message

```
<timestamp>, [FW-1217], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of arbitrated loop physical address (AL_PA) cyclic redundancy check (CRC) errors has fallen below the low boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

A low level of invalid CRC errors means that the switch is functioning normally.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1218

Message

```
<timestamp>, [FW-1218], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of cyclic redundancy check (CRC) errors has risen above the high boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended action

You should configure a five- or six-figure high boundary for this area. Only five-figure (or higher) values for CRC errors indicate problems. When an “above” message is received, check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or

SFP if necessary. Try cleaning the connectors. Check for damage from heat or deterioration from age.

Severity WARNING

FW-1219

Message

```
<timestamp>, [FW-1219], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of cyclic redundancy check (CRC) errors has changed from a value outside of the acceptable range to a value within the acceptable range. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, as only large numbers of messages indicate a problem in this area.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1240

Message

```
<timestamp>, [FW-1240], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) cyclic redundancy check (CRC) errors has changed. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1241

Message

```
<timestamp>, [FW-1241], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) cyclic redundancy check (CRC) errors has fallen below the low boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of CRC errors means that the fabric is functioning normally. The CRC error area of the End-to-End Performance Monitor class helps you tune your fabric. To reduce CRC messages, experiment with alternative topologies and cabling schemes.

Severity INFO

FW-1242

Message

```
<timestamp>, [FW-1242], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) cyclic redundancy check (CRC) errors has risen above the high boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended action The CRC error area of the end-to-end performance monitor class helps the user tune the fabric. To reduce CRC errors, experiment with alternative topologies and cabling schemes. Clean equipment, check temperatures, and replace old hardware.

Severity WARNING

FW-1243

Message

```
<timestamp>, [FW-1243], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) cyclic redundancy check (CRC) errors has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1244

Message

```
<timestamp>, [FW-1244], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) word frames that the switch receives has changed. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1245

Message

```
<timestamp>, [FW-1245], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of end-to-end (EE) word frames that the switch receives has fallen below the low boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1246

Message

```
<timestamp>, [FW-1246], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of end-to-end (EE) word frames that the switch receives has risen above the high boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1247

Message

```
<timestamp>, [FW-1247], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of end-to-end (EE) word frames that the switch receives has changed from a value outside of the acceptable

range to a value within the acceptable range. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1248

Message

```
<timestamp>, [FW-1248], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) word frames that the switch transmits has changed. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1249

Message

```
<timestamp>, [FW-1249], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of end-to-end (EE) word frames that the switch transmits has fallen below the low boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1250

Message

```
<timestamp>, [FW-1250], <sequence-number>,, INFO,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of end-to-end (EE) word frames that the switch transmits has risen above the high boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1251

Message

```
<timestamp>, [FW-1251], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of end-to-end (EE) word frames that the switch transmits has changed from a value outside of the acceptable range to a value within the acceptable range. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1272

Message

```
<timestamp>, [FW-1272], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of frame types or commands that the port receives has changed. The port has received small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1273

Message

```
<timestamp>, [FW-1273], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of frame types or commands that the port receives has fallen below the low boundary. The port has received a small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1274

Message

```
<timestamp>, [FW-1274], <sequence-number>,, INFO,
<system-name>, <Label>, is above high
boundary(High=<Filter Counter>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of frame types or commands that the port receives has risen above the high boundary. The port has received a small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1275

Message

```
<timestamp>, [FW-1275], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of frame types or commands that the port receives has changed from a value outside of the acceptable range to a value within the acceptable range. The port has received a small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1296

Message

```
<timestamp>, [FW-1296], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of telnet violations has changed. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish telnet connections to switches in the fabric.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1297

Message

```
<timestamp>, [FW-1297], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of telnet violations has fallen below the low boundary. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish telnet connections to switches in the fabric.

Recommended action

No action is required.

Severity

INFO

FW-1298

Message

```
<timestamp>, [FW-1298], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of telnet violations has risen above the high boundary. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish telnet connections to switches in the fabric.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1299

Message

```
<timestamp>, [FW-1299], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of telnet violations has changed from a value outside of the acceptable range to a value within the acceptable range. Telnet violations indicate that a telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish telnet connections to switches in the fabric.

Recommended action

No action is required.

Severity

INFO

FW-1300

Message

```
<timestamp>, [FW-1300], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of hypertext transfer protocol (HTTP) violations has changed. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1301

Message

```
<timestamp>, [FW-1301], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of hypertext transfer protocol (HTTP) violations has fallen below the low boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended action

No action is required.

Severity

INFO

FW-1302

Message

```
<timestamp>, [FW-1302], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of hypertext transfer protocol (HTTP) violations has risen above the high boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1303

Message

```
<timestamp>, [FW-1303], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of hypertext transfer protocol (HTTP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended action

No action is required.

Severity

INFO

FW-1304

Message

```
<timestamp>, [FW-1304], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of application programming interface (API) violations has changed. API violations indicate that an API connection request has been received from an unauthorized IP address. The simple network management protocol policy (SNMP_POLICY) contains a list of internet protocol (IP) addresses that are authorized to establish API connections to switches in the fabric.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1305

Message

```
<timestamp>, [FW-1305], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of application programming interface (API) violations has fallen below the low boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The simple network management protocol policy (SNMP_POLICY) contains a list of internet protocol (IP) addresses that are authorized to establish API connections to switches in the fabric.

Recommended action

No action is required.

Severity

INFO

FW-1306

Message

```
<timestamp>, [FW-1306], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of application programming interface (API) violations has risen above the high boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The simple network management protocol policy (SNMP_POLICY) contains a list of internet protocol (IP) addresses that are authorized to establish API connections to switches in the fabric.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1307

Message

```
<timestamp>, [FW-1307], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of application programming interface (API) violations has changed from a value outside of the acceptable range to a value within the acceptable range. API violations indicate that an API connection request has been received from an unauthorized IP address. The simple network management protocol policy (SNMP_POLICY) contains a list of internet protocol (IP) addresses that are authorized to establish API connections to switches in the fabric.

Recommended action

No action is required.

Severity

INFO

FW-1308

Message

```
<timestamp>, [FW-1308], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of simple network management protocol read (RSNMP) violations has changed. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1309

Message

```
<timestamp>, [FW-1309], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of simple network management protocol read (RSNMP) violations has fallen below the low boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended action

No action is required.

Severity

INFO

FW-1310

Message

```
<timestamp>, [FW-1310], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of simple network management protocol read (RSNMP) violations has risen above the high boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1311

Message

```
<timestamp>, [FW-1311], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of simple network management protocol read (RSNMP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended action No action is required.

Severity INFO

FW-1312

Message

```
<timestamp>, [FW-1312], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of simple network management protocol write (WSNMP) violations has changed. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1313

Message

```
<timestamp>, [FW-1313], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of simple network management protocol write (WSNMP) violations has fallen below the low boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended action No action is required.

Severity INFO

FW-1314

Message

```
<timestamp>, [FW-1314], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of simple network management protocol write (WSNMP) violations has risen above the high boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1315

Message

```
<timestamp>, [FW-1315], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of simple network management protocol write (WSNMP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended action No action is required.

Severity INFO

FW-1316

Message

```
<timestamp>, [FW-1316], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of SES violations has changed. SES violations indicate that an small computer system interface (SCSI) Enclosure Services (SES) request has been received from an unauthorized world-wide name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended action

Run the **errShow** command to determine the IP address that sent the request. Responses to security class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1317

Message

```
<timestamp>, [FW-1317], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of SES violations has fallen below the low boundary. SES violations indicate that an small computer system interface (SCSI) Enclosure Services (SES) request has been received from an unauthorized world-wide name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended action

No action is required.

Severity

INFO

FW-1318

Message

```
<timestamp>, [FW-1318], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of SES violations has risen above the high boundary. SES violations indicate that an small computer system interface (SCSI) Enclosure Services (SES) request has been received from an unauthorized world-wide name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1319

Message

```
<timestamp>, [FW-1319], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of SES violations has changed from a value outside of the acceptable range to a value within the acceptable range. SES violations indicate that an small computer system interface (SCSI) Enclosure Services (SES) request has been received from an unauthorized world-wide name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended action

No action is required.

Severity

INFO

FW-1320

Message

```
<timestamp>, [FW-1320], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of simple network management server (MS) violations has changed. MS violations indicate that a MS access request has been received from an unauthorized world-wide name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1321

Message

```
<timestamp>, [FW-1321], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of simple network management server (MS) violations has fallen below the low boundary. MS violations indicate that a MS access request has been received from an unauthorized world-wide name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended action

No action is required.

Severity

INFO

FW-1322

Message

```
<timestamp>, [FW-1322], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of simple network management server (MS) violations has risen above the high boundary. MS violations indicate that a MS access request has been received from an unauthorized world-wide name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1323

Message

```
<timestamp>, [FW-1323], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of simple network management server (MS) violations has changed from a value outside of the acceptable range to a value within the acceptable range. MS violations indicate that a MS access request has been received from an unauthorized world-wide name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended action

No action is required.

Severity

INFO

FW-1324

Message

```
<timestamp>, [FW-1324], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of serial violations has changed. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch world-wide names (WWNs) for which serial port access is enabled.

Recommended action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1325

Message

```
<timestamp>, [FW-1325], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of serial violations has fallen below the low boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch world-wide names (WWNs) for which serial port access is enabled.

Recommended action

No action is required.

Severity

INFO

FW-1326

Message

```
<timestamp>, [FW-1326], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of serial violations has risen above the high boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch world-wide names (WWNs) for which serial port access is enabled.

Recommended action Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1327

Message

```
<timestamp>, [FW-1327], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of serial violations has changed from a value outside of the acceptable range to a value within the acceptable range. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch world-wide names (WWNs) for which serial port access is enabled.

Recommended action No action is required.

Severity INFO

FW-1328

Message

```
<timestamp>, [FW-1328], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of front panel violations has changed. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch world-wide names (WWNs) for which front panel access is enabled.

Recommended action Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1329

Message

```
<timestamp>, [FW-1329], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of front panel violations has fallen below the low boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch world-wide names (WWNs) for which front panel access is enabled.

Recommended action No action is required.

Severity INFO

FW-1330

Message

```
<timestamp>, [FW-1330], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of front panel violations has risen above the high boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch world-wide names (WWNs) for which front panel access is enabled.

Recommended action Run the **errShow** command to determine the Runoff the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1331

Message

```
<timestamp>, [FW-1331], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of front panel violations has changed from a value outside of the acceptable range to a value within the acceptable range. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch world-wide names (WWNs) for which front panel access is enabled.

Recommended action No action is required.

Severity INFO

FW-1332

Message

```
<timestamp>, [FW-1332], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of switch connection control policy (SCC) violations has changed. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world-wide name (WWN) that are allowed to be members of a fabric.

Recommended action Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1333

Message

```
<timestamp>, [FW-1333], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of switch connection control policy (SCC) violations has fallen below the low boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world-wide names (WWNs) that are allowed to be members of a fabric.

Recommended action

No action is required.

Severity

INFO

FW-1334

Message

```
<timestamp>, [FW-1334], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of switch connection control policy (SCC) violations has risen above the high boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world-wide names (WWNs) that are allowed to be members of a fabric.

Recommended action

Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1335

Message

```
<timestamp>, [FW-1335], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of switch connection control policy (SCC) violations has changed from a value outside of the acceptable range to a value within the acceptable range. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world-wide names (WWNs) that are allowed to be members of a fabric.

Recommended action

No action is required.

Severity

INFO

FW-1336

Message

```
<timestamp>, [FW-1336], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of device cable connection (DCC) violations has changed. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the world-wide name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended action

Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

INFO

FW-1337

Message

```
<timestamp>, [FW-1337], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of device cable connection (DCC) violations has fallen below the low boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the world-wide name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended action

No action is required.

Severity

INFO

FW-1338

Message

```
<timestamp>, [FW-1338], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of device cable connection (DCC) violations has risen above the high boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request that the world-wide name ((WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended action

Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend

on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1339

Message

```
<timestamp>, [FW-1339], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of device cable connection (DCC) violations has changed from a value outside of the acceptable range to a value within the acceptable range. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request that the world-wide name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended action No action is required.

Severity INFO

FW-1340

Message

```
<timestamp>, [FW-1340], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of login violations has changed. Login violations indicate that a login failure has been detected.

Recommended action Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1341

Message

```
<timestamp>, [FW-1341], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of login violations has fallen below the low boundary. Login violations indicate that a login failure has been detected.

Recommended action No action is required.

Severity INFO

FW-1342

Message

```
<timestamp>, [FW-1342], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of login violations has risen above the high boundary. Login violations indicate that a login failure has been detected.

Recommended action Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1343

Message

```
<timestamp>, [FW-1343], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of login violations has changed from a value outside of the acceptable range to a value within the acceptable range. Login violations indicate that a login failure has been detected.

Recommended action No action is required.

Severity INFO

FW-1344

Message

```
<timestamp>, [FW-1344], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of invalid timestamps has changed. Invalid-timestamp violations indicate that a packet with an invalid timestamp has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1345

Message

```
<timestamp>, [FW-1345], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of invalid timestamps has fallen below the low boundary. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary world-wide name (WWN). When the primary fabric configuration server (FCS) downloads a new configuration to other switches in the fabric, the

packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended action No action is required.

Severity INFO

FW-1346

Message

```
<timestamp>, [FW-1346], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of invalid timestamps has risen above the high boundary. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1347

Message

```
<timestamp>, [FW-1347], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid timestamps has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid-timestamp violations indicate a packet with an invalid timestamp has been received from the primary fabric configuration

server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended action No action is required.

Severity INFO

FW-1348

Message

```
<timestamp>, [FW-1348], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of invalid signatures has changed. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1349

Message

```
<timestamp>, [FW-1349], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of invalid signatures has fallen below the low boundary. Invalid-signature violations indicate that a packet

with an invalid signature has been received from the primary fabric configuration server (FCS). When the FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended action No action is required.

Severity INFO

FW-1350

Message `<timestamp>, [FW-1350], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable cause Indicates that the number of invalid signatures has risen above the high boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1351

Message `<timestamp>, [FW-1351], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable cause Indicates that the number of invalid signatures has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended action No action is required.

Severity INFO

FW-1352

Message

```
<timestamp>, [FW-1352], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of invalid certificates has changed. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1353

Message

```
<timestamp>, [FW-1353], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of invalid certificates has fallen below the low boundary. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended action

No action is required.

Severity

INFO

FW-1354

Message

```
<timestamp>, [FW-1354], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of invalid certificates has risen above the high boundary. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1355

Message

```
<timestamp>, [FW-1355], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of invalid certificates has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended action No action is required.

Severity INFO

FW-1356

Message

```
<timestamp>, [FW-1356], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of authentication failures has changed. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1357

Message

```
<timestamp>, [FW-1357], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of authentication failures has fallen below the low boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended action No action is required.

Severity INFO

FW-1358

Message

```
<timestamp>, [FW-1358], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of authentication failures has risen above the high boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1359

Message

```
<timestamp>, [FW-1359], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of authentication failures has changed from a value outside of the acceptable range to a value within the acceptable range. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended action No action is required.

Severity INFO

FW-1360

Message

```
<timestamp>, [FW-1360], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of switch link authentication protocol (SLAP) faulty packets has changed. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1361

Message

```
<timestamp>, [FW-1361], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of switch link authentication protocol (SLAP) faulty packets has fallen below the low boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended action

No action is required.

Severity

INFO

FW-1362

Message

```
<timestamp>, [FW-1362], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of switch link authentication protocol (SLAP) faulty packets has risen above the high boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1363

Message

```
<timestamp>, [FW-1363], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of switch link authentication protocol (SLAP) faulty packets has changed from a value outside of the acceptable range to a value within the acceptable range. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended action No action is required.

Severity INFO

FW-1364

Message

```
<timestamp>, [FW-1364], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of time service (TS) out-of-sync violations has changed.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1365

Message

```
<timestamp>, [FW-1365], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of time service (TS) out-of-sync violations has fallen below the low boundary.

Recommended action No action is required.

Severity INFO

FW-1366

Message

```
<timestamp>, [FW-1366], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of time service (TS) out-of-sync violations has risen above the high boundary.

Recommended action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity

WARNING

FW-1367

Message

```
<timestamp>, [FW-1367], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the number of time service (TS) out-of-sync violations has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended action

No action is required.

Severity

INFO

FW-1368

Message

```
<timestamp>, [FW-1368], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause

Indicates that the number of no-FCS violations has changed. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate

to a switch, the receiving switch saves the world-wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1369

Message

```
<timestamp>, [FW-1369], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of no-FCS violations has fallen below the low boundary. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world-wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended action No action is required.

Severity INFO

FW-1370

Message

```
<timestamp>, [FW-1370], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of no-FCS violations has risen above the high boundary. This counter records how often the switch loses

contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world-wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1371

Message

```
<timestamp>, [FW-1371], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of no-FCS violations has changed from a value outside of the acceptable range to a value within the acceptable range. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world-wide name WWN of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended action No action is required.

Severity INFO

FW-1372

Message

```
<timestamp>, [FW-1372], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of incompatible security database violations has changed. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1373

Message

```
<timestamp>, [FW-1373], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of incompatible security database violations has fallen below the low boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended action No action is required.

Severity INFO

FW-1374

Message

```
<timestamp>, [FW-1374], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of incompatible security database violations has risen above the high boundary. This violation indicates

the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1375

Message

```
<timestamp>, [FW-1375], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of incompatible security database violations has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended action No action is required.

Severity INFO

FW-1376

Message

```
<timestamp>, [FW-1376], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of illegal commands has changed. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed

on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1377

Message

```
<timestamp>, [FW-1377], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of illegal commands has fallen below the low boundary. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended action No action is required.

Severity INFO

FW-1378

Message

```
<timestamp>, [FW-1378], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the number of illegal commands has risen above the high boundary. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch

have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1379

Message

```
<timestamp>, [FW-1379], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause Indicates that the number of illegal commands has changed from a value outside of the acceptable range to a value within the acceptable range. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended action No action is required.

Severity INFO

FW-1400

Message

```
<timestamp>, [FW-1400], <sequence-number>,, INFO,
<system-name>, <Label>, value has changed(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the flash usage percentage has changed. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1401

Message

```
<timestamp>, [FW-1401], <sequence-number>,, INFO,
<system-name>, <Label>, is below low boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the flash usage percentage has fallen below the low boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1402

Message

```
<timestamp>, [FW-1402], <sequence-number>,, WARNING,
<system-name>, <Label>, is above high boundary(High=<High
value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable cause Indicates that the flash usage percentage has risen above the high boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended action You might have to remove some unwanted files to create some flash space. Run the **supportSave** command to remove files from the kernel space.

Severity WARNING

FW-1403

Message

```
<timestamp>, [FW-1403], <sequence-number>,, INFO,
<system-name>, <Label>, is between high and low
boundaries(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable cause

Indicates that the flash usage percentage has changed from a value outside of the acceptable range to a value within the acceptable range. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity

INFO

FW-1424

Message

```
<timestamp>, [FW-1424], <sequence-number>,, WARNING,
<system-name>, Switch status changed from <Previous
state> to <Current state>.
```

Probable cause

Indicates that the switch status is not in a healthy state. This occurred because of a policy violation.

Recommended action

Run the **switchStatusShow** command to determine the policy violation.

Severity

WARNING

FW-1425

Message

```
<timestamp>, [FW-1425], <sequence-number>,, INFO,
<system-name>, Switch status changed from <Bad state> to
HEALTHY.
```

Probable cause

Indicates that the switch status has changed to a healthy state. This occurred because a policy is no longer violated.

Recommended action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1426

Message
```
<timestamp>, [FW-1426], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Power supply: <Number Bad> bad, <Number Missing> absent.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty or missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended action Replace the faulty or missing power supply.

Severity WARNING

FW-1427

Message
```
<timestamp>, [FW-1427], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Power supply: <Number Bad> bad.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended action Replace the faulty power supply.

Severity WARNING

FW-1428

Message
```
<timestamp>, [FW-1428], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Power supply: <Number Missing> absent.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended action Replace the missing power supply.

Severity WARNING

FW-1429

Message

```
<timestamp>, [FW-1429], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor:
Power supplies are not redundant.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the power supplies are not in the correct slots for redundancy.

Recommended action Rearrange the power supplies so that one is in an odd slot and other in an even slot to make them redundant.

Severity WARNING

FW-1430

Message

```
<timestamp>, [FW-1430], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
<string>.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty temperature sensors is greater than or equal to the policy set by the **switchStatusPolicySet** command. A temperature sensor is faulty when the sensor value is not in the acceptable range or is faulty.

Recommended action Replace the field-replaceable unit (FRU) with the faulty temperature sensor.

Severity WARNING

FW-1431

Message

```
<timestamp>, [FW-1431], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Fan: <Number Bad> bad.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty fans is greater than or equal to the policy set by the **switchStatusPolicySet** command. A fan is faulty when sensor value is not in the acceptable range or is faulty.

Recommended action Replace the faulty or deteriorating fan field-replaceable units (FRUs).

Severity WARNING

FW-1432

Message

```
<timestamp>, [FW-1432], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
WWN: <Number Bad> bad.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty world-wide name (WWN) cards is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended action Replace the faulty WWN card.

Severity WARNING

FW-1433

Message

```
<timestamp>, [FW-1433], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
CP: CP non-redundant.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty CPs is greater than or equal to the policy set by the **switchStatusPolicySet** command. The CPs are non-redundant.

Recommended action Run the **firmwareShow** command to verify that both CPs have compatible firmware levels. Run the **firmwareDownload** command to to install the same level of firmware to both CPs. Replace any faulty CPs.

If you reset the micro-switch (the latch on the CP blade) on the active CP before the heartbeat was up on a power cycle, and the CPs came

up non-redundant, then you should reboot the CPs again to clear the problem.

Severity WARNING

FW-1434

Message

```
<timestamp>, [FW-1434], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Blade: <Number Bad> blade failures.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended action Replace the faulty blade.

Severity WARNING

FW-1435

Message

```
<timestamp>, [FW-1435], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Flash: usage out of range.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the flash usage is out of range. The policy was set using the **switchStatusPolicySet** command.

Recommended action Run the **supportSave** command to clear out the kernel flash.

Severity WARNING

FW-1436

Message

```
<timestamp>, [FW-1436], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Marginal ports: <Num of marginal ports and the port
numbers> marginal ports. (Port(s) <Unknown>)
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of marginal ports is greater than or equal to the policy set using the **switchStatusPolicySet** command. A port is faulty when the port value for Link Loss, Synchronization Loss, Signal Loss, Invalid word, Protocol error, cyclic redundancy check (CRC) error, Port state change or Buffer Limited Port is above the high boundary.

Recommended action Replace any faulty or deteriorating small form-factor pluggables (SFPs).

Severity WARNING

FW-1437

Message

```
<timestamp>, [FW-1437], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
faulty ports: <Num of faulty ports>. (Port(s) <unknown>.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty ports is greater than or equal to the policy set by the **switchStatusPolicySet** command. A port is considered faulty due to hardware failure such as a faulty small form-factor pluggable (SFP) or port.

Recommended action Replace any faulty or deteriorating small form-factor pluggables (SFPs).

Severity WARNING

FW-1438

Message

```
<timestamp>, [FW-1438], <sequence-number>,, WARNING,
<system-name>, Switch status change contributing factor
Missing SFPs: <Num of missing SFPs> missing SFPs.
```

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the number of missing small form-factor pluggables (SFPs) is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended action Run the **switchStatusPolicySet** command to modify the SFP policy or to add SFPs to the empty ports.

Severity WARNING

FW-1439

Message `<timestamp>, [FW-1439], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Switch offline.`

Probable cause Indicates that the switch status is not in a healthy state. This occurred because the switch is offline.

Recommended action Run the **switchEnable** command.

Severity WARNING

FW-1440

Message `<timestamp>, [FW-1440], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “absent”.

Recommended action No action is required. Verify that the event was planned.

Severity INFO

FW-1441

Message `<timestamp>, [FW-1441], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “inserted”. This means that an FRU is inserted but not powered on.

Recommended action No action is required. Verify that the event was planned.

Severity INFO

FW-1442

Message `<timestamp>, [FW-1442], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “on”.

Recommended action No action is required. Verify that the event was planned.

Severity INFO

FW-1443

Message `<timestamp>, [FW-1443], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable cause Indicates that the state of the specified field-replaceable unit (FRU) changed to “off”.

Recommended action No action is required. Verify that the event was planned.

Severity INFO

FW-1444

Message `<timestamp>, [FW-1444], <sequence-number>,, WARNING, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “faulty”.

Recommended action Replace the FRU.

Severity WARNING

FW-1445

Message

```
<timestamp>, [FW-1445], <sequence-number>,, INFO,
<system-name>, Four power supplies are now required for
2X redundancy, Switch Status Policy values changed.
```

Probable cause

Indicates that the switch now requires 4 power supplies and previous Switch Status Policy parameters will be overwritten to reflect this. The presence of an AP blade means that more than one power supply may be required to provide adequate power. So (even if the AP blade is powered down or removed) the Switch Status policy values will now reflect the need for 4 power supplies to maintain full (2X) redundancy.

Recommended action

No action required, unless there are fewer than 4 power supplies active in the chassis. If there are fewer than 4, insert additional power supplies so that there are 4 active.

Severity

INFO

FW-1446

Message

```
<timestamp>, [FW-1446], <sequence-number>,, WARNING,
<system-name>, Four power supplies now required for 2X
redundancy, not enforced by Fabric Watch due to Switch
Status Policy overridden by User.
```

Probable cause

Indicates that the switch now requires 4 power supplies for full (2X) redundancy, but the user has previously overridden the Switch Status Policy values pertaining to number of power supplies. So those values will not be automatically changed. The default values with no AP blades are: 3 out of service indicates switch status is DOWN, 0 indicates no checking for switch status MARGINAL. The default values when an AP blade is or has been present are: 2 out of service indicates switch status is DOWN, 1 out of service indicates switch status is MARGINAL .

Recommended action

To maintain full (2X) redundancy and proper monitoring by Fabric Watch, 4 active power supplies should be supplied and the default values associated with the presence of an AP blade should be entered with **switchStatusPolicyset**.

Severity

WARNING

FW-1500

Message

```
<timestamp>, [FW-1500], <sequence-number>,, WARNING,
<system-name>, Mail overflow - Alerts being discarded.
```

Probable cause

Indicates that mail alert overflow condition has occurred.

Recommended action

Resolve or disable the mail alert using the **fwMailCfg** command.

Severity

WARNING

FW-1501

Message

```
<timestamp>, [FW-1501], <sequence-number>,, INFO,
<system-name>, Mail overflow cleared - <Mails discarded>
alerts discarded.
```

Probable cause

Indicates that the mail overflow condition has cleared.

Recommended action

No action is required.

Severity

INFO

FW-1510

Message

```
<timestamp>, [FW-1510], <sequence-number>,, INFO,
<system-name>, <Area string> threshold exceeded: Port
<Port number> disabled.
```

Probable Cause

Link failures indicates that the specified port is now disabled because the link on this port had multiple link failures that exceed the Fabric Watch threshold on the port. Both physical and hardware problems can cause link failures. Link failures frequently occur due to a loss of synchronization. Link failures also occur due to hardware failures, a defective small form-factor pluggable (SFP) or faulty cable.

Protocol errors indicates CRC sum disparity. Occasionally, these errors occur due to software issues. Persistent errors occur due to hardware problems.

Recommended Action Check for concurrent loss of synchronization errors. Check the SFP and the cable. Replace and faulty or deteriorating cables or SFPs. Then enable the port using the **portEnable** command.

Severity INFO

35

HAM System Messages

This chapter contains information on the following HAM messages:

- HAM-1001 466
- HAM-1002 466
- HAM-1004 466
- HAM-1005 467
- HAM-1006 468
- HAM-1007 468
- HAM-1008 469
- HAM-1009 469

HAM-1001

Message

```
<timestamp>, [HAM-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, Standby CP is not healthy,
device <device name> status BAD, Severity = <Log="YES"
Class="NONE" Severity>
```

Probable cause

Indicates that a standby control processor (CP) device error is reported by the high-availability manager (HAM) Health Monitor, with a specific device and Log="YES" Class="NONE" Severity level. The *severity level* can be "critical", "major", or "minor".

The active CP will continue to function normally, but because the standby CP is not healthy, non-disruptive failover is not possible.

Recommended action

Reboot the standby CP blade by ejecting the card and reseating it.

If the problem persists, replace the standby CP.

Severity

CRITICAL

HAM-1002

Message

```
<timestamp>, [HAM-1002], <sequence-number>,, INFO,
<system-name>, Standby CP is healthy.
```

Probable cause

Indicates that all of the standby control processor (CP) devices monitored by the high-availability manager (HAM) Health Monitor report no error.

Recommended action

No action is required.

Severity

INFO

HAM-1004

Message

```
<timestamp>, [HAM-1004], <sequence-number>,, INFO,
<system-name>, Processor rebooted - <Reboot Reason>.
```

Probable cause

This message records switch processor reboot reasons that were initiated by the user or the switch errors. The switch processor reboots can be initiated by the **firmwareDownload**, **fastBoot**,

haFailover, and **reboot** commands. Some examples of errors that might initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The *reboot reasons* can be any of the following:

- Hafailover
- Unknown
- Fastboot
- Giveup Master:SYSM
- CP Faulty:SYSM
- FirmwareDownload
- ConfigDownload:MS
- ChangeWWN:EM
- Reboot:WebTool
- Fastboot:WebTool
- Software Fault:Software Watchdog
- Software Fault:Kernel Panic
- Software Fault:ASSERT
- Reboot:SNMP
- Fastboot:SNMP
- Reboot
- Chassis Config
- Reboot:API
- Reboot:HAM
- EMFault:EM

Recommended action Check the error log on both CPs for additional messages that might indicate the reason for the reboot.

Severity INFO

HAM-1005

Message

```
<timestamp>, [HAM-1005], <sequence-number>,, INFO,
<system-name>, HeartBeat Miss reached threshold.
```

Probable cause Indicates that either the Active CP EMAC controller or standby CP is down. The active CP will run diagnostic test on the EMAC controller and will wait for the standby CP to reset it if it is down.

Recommended action No action is required.

Severity INFO

HAM-1006

Message `<timestamp>, [HAM-1006], <sequence-number>,, CRITICAL, <system-name>,EMAC controller for Active CP is BAD.`

Probable cause Indicates that the local EMAC controller on the active control processor (CP) is BAD as determined by the diagnostic test run by the ham module.

Recommended action The standby CP will take over and reset the active CP. The system will be non-redundant as the standby becomes the active CP.

Severity CRITICAL

HAM-1007

Message `<timestamp>, [HAM-1007], <sequence-number>,, CRITICAL, <system-name>,Need to reboot the system for recovery, reason: <reason name>.`

Probable Cause Indicates that the system in its current condition needs to be rebooted to achieve a reliable recovery. The reasons can be that the standby CP is not ready when failover occurred, failover happened when the last LS transaction is incomplete, or the system failed when a timeout occurred at a certain stage or cold/warm recovery failed. If auto-reboot is enabled, the system will automatically reboot itself. Otherwise you need to manually reboot it.

Recommended Action For a reliable recovery, reboot the system manually if auto-reboot recovery is disabled.

Severity CRITICAL

HAM-1008

Message

```
<timestamp>, [HAM-1008], <sequence-number>,, CRITICAL,
<system-name>,Rebooting the system for recovery -
auto-reboot is enabled.
```

Probable Cause

Recovery by reboot is enabled, the system will automatically reboot itself. This follows if the event logged in HAM-1007 has happened and auto-reboot is enabled.

Recommended Action

No action is required.

Severity

CRITICAL

HAM-1009

Message

```
<timestamp>, [HAM-1009], <sequence-number>,, CRITICAL,
<system-name>,Need to MANUALLY REBOOT the system for
recovery - auto-reboot is disabled.
```

Probable Cause

Recovery by reboot is disabled, the system needs to be manually rebooted for recovery. This follows if the event logged in HAM-1007 has happened and auto-reboot is disabled.

Recommended Action

Reboot the whole system manually to recover.

Severity

CRITICAL

36

HAMK System Messages

This chapter contains information on the following HAMK messages:

- HAMK-1001 472
- HAMK-1002 472
- HAMK-1003 472
- HAMK-1004 473

HAMK-1001

Message

```
<timestamp>, [HAMK-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, Warm recovery failed.
```

Probable cause

The switch failed in the warm recovery.

Recommended action

This message triggers a switch reboot automatically and attempts a cold recovery. Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

HAMK-1002

Message

```
<timestamp>, [HAMK-1002], <sequence-number>,, INFO,
<system-name>, Heartbeat down.
```

Probable cause

Indicates that the active control processor (CP) blade determined that the standby CP blade is down. This can be a result of an operator-initiated action such as **firmwareDownload**, the standby CP blade being reset or removed, or as a result of an error in the standby CP blade.

Recommended action

Monitor the standby CP blade for a few minutes. If this message is due to a standby CP reboot, the message HAMK-1003 will display after the standby CP has completed the reboot successfully.

If the standby CP does not successfully connect to the active CP after 10 minutes, reboot the standby CP blade by ejecting the blade and reseating it.

Severity

INFO

HAMK-1003

Message

```
<timestamp>, [HAMK-1003], <sequence-number>,, INFO,
<system-name>, Heartbeat up.
```

Probable cause

Indicates that the active control processor (CP) blade detects the standby CP blade. This message indicates that the standby CP blade

is available to take over in case a failure happens on the active CP blade. This message is typically seen when the standby CP blade reboots.

Recommended action No action is required. This message means that the standby CP is healthy.

Severity INFO

HAMK-1004

Message `<timestamp>,[HAMK-1004], <sequence-number>,, INFO, <system-name>, Resetting standby CP (double reset may occur).`

Probable cause Indicates that the standby control processor (CP) is being reset due to a loss of heartbeat. This message is typically seen when the standby CP has been rebooted. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

Recommended action No action is required.

Severity INFO

37

HIL System Messages

This chapter contains information on the following HIL messages:

- HIL-1101 477
- HIL-1102 477
- HIL-1103 477
- HIL-1104 478
- HIL-1105 478
- HIL-1106 478
- HIL-1107 479
- HIL-1108 479
- HIL-1201 480
- HIL-1202 480
- HIL-1203 481
- HIL-1204 481
- HIL-1206 482
- HIL-1207 482
- HIL-1208 483
- HIL-1301 483
- HIL-1302 483
- HIL-1303 484
- HIL-1304 484
- HIL-1305 484
- HIL-1306 485
- HIL-1307 485
- HIL-1308 485
- HIL-1309 486
- HIL-1310 486
- HIL-1311 486
- HIL-1401 487

- HIL-1402 487
- HIL-1403 487
- HIL-1404 488
- HIL-1501 488
- HIL-1502 488
- HIL-1503 489
- HIL-1504 489
- HIL-1505 490
- HIL-1506 490
- HIL-1507 491
- HIL-1508 491
- HIL-1509 492
- HIL-1510 492
- HIL-1601 493
- HIL-1602 493
- HIL-1603 493
- HIL-1610 494
- HIL-1650 494

HIL-1101

Message

```
<timestamp>, [HIL-1101], <sequence-number>,, ERROR,
<system-name>, Slot <slot number> faulted, <nominal
voltage> (<measured voltage>) is above threshold.
```

Probable cause Indicates that the blade voltage is above the threshold.

Recommended action Replace the faulty blade or switch (for nonbladed switches).

Severity ERROR

HIL-1102

Message

```
<timestamp>, [HIL-1102], <sequence-number>,, ERROR,
<system-name>, Slot <slot number> faulted, <nominal
voltage> (<measured voltage>) is below threshold.
```

Probable cause Indicates that the blade voltage is below the threshold.

Recommended action Replace the faulty blade or switch (for nonbladed switches).

Severity ERROR

HIL-1103

Message

```
<timestamp>, [HIL-1103], <sequence-number>,, ERROR,
<system-name>, Blower <blower number> faulted, <nominal
voltage> (<measured voltage>) is above threshold.
```

Probable cause Indicates that the fan voltage is above threshold.

Recommended action Run the **psShow** command to verify the power supply status.

Try to reseat the faulty fan field-replaceable unit (FRU) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

Severity ERROR

HIL-1104

Message

```
<timestamp>, [HIL-1104], <sequence-number>,, ERROR,
<system-name>, Blower <blower number> faulted, <nominal
voltage> (<measured voltage>) is below threshold.
```

Probable cause

Indicates that the fan voltage is below the threshold.

Recommended action

Run the **psShow** command to verify the power supply status.

Try to reseat the faulty fan field-replaceable unit (FRU) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

Severity

ERROR

HIL-1105

Message

```
<timestamp>, [HIL-1105], <sequence-number>,, ERROR,
<system-name>, Switch error, <nominal voltage> (<measured
voltage>) above threshold.
```

Probable cause

Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the enterprise-class platforms.

Recommended action

For the DS-220B and DS-300B, the entire switch must be replaced, because these switches do not have field-replaceable units (FRUs).

For all others, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity

ERROR

HIL-1106

Message

```
<timestamp>, [HIL-1106], <sequence-number>,, ERROR,
<system-name>, Switch error, <nominal voltage> (<measured
voltage>) below threshold.
```

Probable cause Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to enterprise-class platforms.

Recommended action For the DS-220B and DS-300B, the entire switch must be replaced, because these switches do not have field-replaceable units (FRUs).

For all others, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity ERROR

HIL-1107

Message

```
<timestamp>, [HIL-1107], <sequence-number>,, ERROR,
<system-name>, Switch faulted, <nominal voltage>
(<measured voltage>)above threshold.
```

Probable cause Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to enterprise-class platforms.

Recommended action For the DS-220B and DS-300B, the entire switch must be replaced, because these switches do not have field-replaceable units (FRUs).

For all others, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity ERROR

HIL-1108

Message

```
<timestamp>, [HIL-1108], <sequence-number>, FFDC,
CRITICAL, <system-name>, Switch faulted, <nominal
voltage> (<measured voltage>) below threshold. System
preparing for reset.
```

Probable cause Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to enterprise-class platforms.

Recommended action For the DS-220B and DS-300B, the entire switch must be replaced, because these switches do not have field-replaceable units (FRUs).

For all others, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity CRITICAL

HIL-1201

Message

```
<timestamp>, [HIL-1201], <sequence-number>,, WARNING<
<system-name>, Blower <blower number>, speed (<measured
speed> RPM) above threshold.
```

Probable cause Indicates that the fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended action Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan field-replaceable unit (FRU).

Severity WARNING

HIL-1202

Message

```
<timestamp>, [HIL-1202], <sequence-number>,, ERROR,
<system-name>, Blower <blower number> faulted, speed
(<measured speed> RPM) below threshold.
```

Probable cause Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold.

Recommended action Replace the fan field-replaceable unit (FRU).

Severity ERROR

HIL-1203

Message

```
<timestamp>, [HIL-1203], <sequence-number>,, ERROR,
<system-name>, Fan <fan number> faulted, speed (<measured
speed> RPM) above threshold.
```

Probable cause

Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended action

Run the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan field-replaceable unit (FRU).

Severity

ERROR

HIL-1204

Message

```
<timestamp>, [HIL-1204], <sequence-number>,, ERROR,
<system-name>, Fan <fan number> faulted, speed (<measured
speed> RPM) below threshold.
```

Probable cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This message is specific to nonbladed switches and is not applicable to enterprise-class platforms.

Recommended action

For the DS-220B and DS-300B, the entire switch must be replaced, because these switches do not have field-replaceable units (FRUs).

For all others, replace the fan field-replaceable unit (FRU).

Severity

ERROR

HIL-1206

Message

```
<timestamp>, [HIL-1206], <sequence-number>,, ERROR,
<system-name>, Fan <fan number> sensor <sensor number> ,
speed (<measured speed> RPM) below threshold.
```

Probable cause

Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to nonbladed switches and is not applicable to enterprise-class platforms.

Recommended action

For the DS-220B and DS-300B, the entire switch must be replaced, because these switches do not have field-replaceable units (FRUs).

For all others, replace the fan field-replaceable unit (FRU).

Severity

ERROR

HIL-1207

Message

```
<timestamp>, [HIL-1207], <sequence-number>,, ERROR,
<system-name>, Fan <fan number> is faulty.
```

Probable cause

Indicates that the fan is faulty.

Recommended action

Use the **tempShow** command to verify that the switch temperatures are within operational range. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Use the **fanShow** command to monitor the status of the fan generating this error.

If the fan continues to generate this message, replace the switch because the fan is not field-replaceable.

Severity

ERROR

HIL-1208

Message

```
<timestamp>, [HIL-1208], <sequence-number>,, INFO,
<system-name>, Fan <fan number> is not faulty.
```

Probable cause

Indicates that the fan is not faulty.

Recommended action

This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

Severity

INFO

HIL-1301

Message

```
<timestamp>, [HIL-1301], <sequence-number>,, WARNING,
<system-name>, 1 blower failed or missing. Replace failed
or missing blower assembly immediately.
```

Probable cause

Indicates that a fan field-replaceable unit (FRU) has failed or has been removed. This message is often preceded by a low speed error message. This problem can cause the switch to overheat.

Recommended action

Replace the affected fan FRU immediately.

Severity

WARNING

HIL-1302

Message

```
<timestamp>, [HIL-1302], <sequence-number>,, WARNING,
<system-name>, <count> blowers failed or missing. Replace
failed or missing blower assemblies immediately.
```

Probable cause

Indicates that multiple fan field-replaceable unit (FRU)s have failed or are missing on a switch. This message is often preceded by a low fan speed message.

Recommended action

Replace the affected fan FRUs immediately.

Severity WARNING

HIL-1303

Message `<timestamp>, [HIL-1303], <sequence-number>,, ERROR, <system-name>, One fan failed. Replace failed fan FRU immediately.`

Probable cause Indicates that a fan field-replaceable unit (FRU) has failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan FRU immediately.

Severity ERROR

HIL-1304

Message `<timestamp>, [HIL-1304], <sequence-number>,, ERROR, <system-name>, Two fans failed. Replace failed fan FRUs immediately.`

Probable cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1305

Message `<timestamp>, [HIL-1305], <sequence-number>,, ERROR, <system-name>, One or two fan(s) failed. Replace failed fan FRUs immediately.`

Probable cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1306

Message

```
<timestamp>, [HIL-1306], <sequence-number>,, ERROR,
<system-name>, Three fans failed. Replace failed fan FRUs
immediately.
```

Probable cause Indicates that three fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1307

Message

```
<timestamp>, [HIL-1307], <sequence-number>,, ERROR,
<system-name>, Four or five fans failed. Replace failed
fan FRUs immediately.
```

Probable cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1308

Message

```
<timestamp>, [HIL-1308], <sequence-number>,, ERROR,
<system-name>, All fans failed. Replace failed fan FRUs
immediately.
```

Probable cause Indicates that all fans have failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan field-replaceable units (FRUs) immediately.

Severity ERROR

HIL-1309

Message

```
<timestamp>, [HIL-1309], <sequence-number>,, ERROR,
<system-name>, <count> fan FRUs failed. Replace failed
fan FRUs immediately.
```

Probable cause Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended action Replace the faulty fan field-replaceable unit (FRU)s immediately.

Severity ERROR

HIL-1310

Message

```
<timestamp>, [HIL-1310], <sequence-number>,, WARNING,
<system-name>, <count> fan(s) faulty.
```

Probable cause Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended action Since the fans are not field replaceable, replace the switch if the temperature is high.

Severity WARNING

HIL-1311

Message

```
<timestamp>, [HIL-1311], <sequence-number>,, INFO,
<system-name>, No fans are faulty.
```

Probable cause Indicates recovery from earlier condition of one or more fans having failed.

Recommended action This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

Severity INFO

HIL-1401

Message

```
<timestamp>, [HIL-1401], <sequence-number>,, WARNING,
<system-name>, One fan FRU missing. Install fan FRU
immediately.
```

Probable cause Indicates that one fan field-replaceable unit (FRU) has been removed.

Recommended action Install the missing fan FRU.

Severity WARNING

HIL-1402

Message

```
<timestamp>, [HIL-1402], <sequence-number>,, WARNING,
<system-name>, Two fan FRUs missing. Install fan FRUs
immediately.
```

Probable cause Indicates that two fan field-replaceable units (FRUs) have been removed.

Recommended action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1403

Message

```
<timestamp>, [HIL-1403], <sequence-number>,, WARNING,
<system-name>, All fan FRUs missing. Install fan FRUs
immediately.
```

Probable cause Indicates that all fan field-replaceable units (FRUs) have been removed.

Recommended action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1404

Message

```
<timestamp>, [HIL-1404], <sequence-number>,, WARNING,
<system-name>, <count> fan FRUs missing. Install fan FRUs
immediately.
```

Probable cause

Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended action

Install the missing fan FRUs immediately.

Severity

WARNING

HIL-1501

Message

```
<timestamp>, [HIL-1501], <sequence-number>,, WARNING,
<system-name>, Slot <slot number>, high temperature
(<measured temperature>).
```

Probable cause

Indicates that the temperature of this blade has risen above the warning threshold.

Recommended action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

WARNING

HIL-1502

Message

```
<timestamp>, [HIL-1502], <sequence-number>, FFDC,
CRITICAL, <system-name>, Slot <slot number>, high
temperature (<measured temperature>). Unit will be shut
down in 2 minutes if temperature remains high.
```

Probable cause

Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message.

Recommended action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

Severity

CRITICAL

HIL-1503

Message

```
<timestamp>, [HIL-1503], <sequence-number>, FFDC,
CRITICAL, <system-name>, Slot <slot number>, unit
shutting down.
```

Probable cause

Indicates that the temperature of this blade has risen above the maximum threshold for at least two minutes. The blade is shut down to prevent further damage. This usually follows a high-temperature warning message.

Recommended action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

Severity

CRITICAL

HIL-1504

Message

```
<timestamp>, [HIL-1504], <sequence-number>,, INFO,
<system-name>, System within normal temperature
specifications (<measured temperature> C).
```

Probable cause

Indicates that temperatures in the system have returned to normal.

Recommended action

No action is required.

Severity INFO

HIL-1505

Message `<timestamp>, [HIL-1505], <sequence-number>,, WARNING, <system-name>, High temperature (<measured temperature> C) exceeds environmental specifications.`

Probable cause Indicates that temperatures in the system have risen above the warning threshold.

Recommended action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity WARNING

HIL-1506

Message `<timestamp>, [HIL-1506], <sequence-number>, FFDC, CRITICAL, <system-name>, High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down within 2 minutes.`

Probable cause Indicates that temperatures in the system have risen above the critical threshold.

Recommended action Run the **fanShow** command to verify that all fans are working properly. Replace any deteriorating fan field-replaceable units (FRUs).

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity CRITICAL

HIL-1507

Message

```
<timestamp>, [HIL-1507], <sequence-number>, FFDC,
CRITICAL, <system-name>, High temperature warning time
expired. System preparing for shutdown.
```

Probable cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended action

In order to avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1508

Message

```
<timestamp>, [HIL-1508], <sequence-number>, FFDC,
CRITICAL, <system-name>, Fan faulty warning time expired.
System preparing for shutdown.
```

Probable cause

Indicates that temperatures in the system have remained above the critical threshold too long.

Recommended action

In order to avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1509

Message

```
<timestamp>, [HIL-1509], <sequence-number>, FFDC,
CRITICAL, <system-name>, High temperature (<measured
temperature> C). Warning time expired. System preparing
for shutdown.
```

Probable cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended action

In order to avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

CRITICAL

HIL-1510

Message

```
<timestamp>, [HIL-1510], <sequence-number>,, WARNING,
<system-name>, Current temperature (<measured
temperature> C) is below shutdown threshold. System
shutdown cancelled.
```

Probable cause

Indicates that temperatures in the system have dropped below the critical threshold, so that the system can continue operation.

Recommended action

To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity

WARNING

HIL-1601

Message

```
<timestamp>, [HIL-1601], <sequence-number>,, ERROR,
<system-name>, Using backup temperature sensor. Service
immediately.
```

Probable cause

Indicates that temperature readings from the primary sensor are out of range.

Recommended action

Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs).

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

Severity

ERROR

HIL-1602

Message

```
<timestamp>, [HIL-1602], <sequence-number>, FFDC,
CRITICAL, <system-name>, Multiple temperature sensors
failed. Service immediately.
```

Probable cause

Indicates that temperature readings from multiple sensors are out of range.

Recommended action

Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs).

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

Severity

CRITICAL

HIL-1603

Message

```
<timestamp>, [HIL-1602], <sequence-number>, FFDC,
CRITICAL, <system-name>, <failure count> fans out of
service. System is shutting down immediately.
```

Probable cause Indicates that total fan failure count is greater than or equal to two.

Recommended action In order to avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Severity CRITICAL

HIL-1610

Message

```
<timestamp>, [HIL-1610], <sequence-number>, FFDC,
WARNING, <system-name>, Fan/PS unit <Combo fan/power
supply unit number> not supplying power, fan speeds not
available. Please ensure that the unit has power and the
switch is on.
```

Probable Cause Indicates that the power supply is not connected to a power source , it is not switched on, or the unit is faulty. Applicable only to the DS-5100B.

Recommended Action Ensure the power cord is connected to the unit with a valid power source and then switch on the unit. If the problem persists, try reseating the unit. If the problem still persists replace the FRU.

Severity WARNING

HIL-1650

Message

```
<timestamp>, [HIL-1650], <sequence-number>,, ERROR,
<system-name>, <failure count> unable to detect both WWN
cards in chassis. Access to WWN halted.
```

Probable cause One or both of the WWN cards is missing. Both WWN cards must be present for normal operation.

Recommended action Make sure both WWN cards are inserted.

Severity ERROR

38

HLO System Messages

This chapter contains information on the following HLO messages:

- HLO-1001 496
- HLO-1002 496
- HLO-1003 497

HLO-1001

Message

```
<timestamp>, [HLO-1001], <sequence-number>, FFDC, ERROR,
<system-name>, Incompatible Inactivity timeout <dead
timeout> from port <port number>, correct value <value>.
```

Probable cause

Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The Connectrix B switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO dead timeout value is not configurable, so this error can only occur when the Connectrix B switch is connected to a switch from another manufacturer.

Recommended action

The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to documentation of the other manufacturer's switch to change this value.

Severity

ERROR

HLO-1002

Message

```
<timestamp>, [HLO-1002], <sequence-number>, FFDC, ERROR,
<system-name>, Incompatible Hello timeout <HLO timeout>
from port <port number>, correct value <correct value>.
```

Probable cause

Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The Connectrix B switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO timeout value is not configurable, so this error can only occur when the Connectrix B switch is connected to a switch from another manufacturer.

Recommended action

The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to documentation of the other manufacturer's switch to change this value.

Severity

ERROR

HLO-1003

Message

```
<timestamp>, [HLO-1003], <sequence-number>, FFDC, ERROR,
<system-name>, Invalid Hello received from port <port
number>, Domain = <domain ID>, Remote Port =<remote port
ID>.
```

Probable cause

Indicates that the HLO message received was invalid and the frame was dropped. The Connectrix B switch will not accept FSPF frames from the remote switch.

The switch has received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can only occur when the Connectrix B switch is connected to a switch from another manufacturer.

Recommended action

The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to documentation of the other manufacturer's switch to change this value.

Severity

ERROR

39

HMON System Messages

This chapter contains information on the following HMON message:

- HMON-1001 500

HMON-1001

Message

```
<timestamp>, [HMON-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, <Failure description>
```

Probable cause

Indicates that there was a problem reading an essential file containing configuration information from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware to your switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

40

HTTP System Messages

This chapter contains information on the following HTTP messages:

- HTTP-1001 502
- HTTP-1002 502
- HTTP-1003 502

HTTP-1001

Message `<timestamp>, [HTTP-1001], <sequence-number>,, INFO, <system-name>, Switch PIDformat has changed to <current PID format>.`

Probable cause Indicates that the PID format was changed by the administrator.

Recommended action No action is required. For more information on PID, format refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide*.

Severity INFO

HTTP-1002

Message `<timestamp>, [HTTP-1002], <sequence-number>, AUDIT, INFO, <system-name>, Zoning transaction initiated by User: <User Name>, Role: <User Role> completed successfully.`

Probable cause Indicates that the zoning database has been changed.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

HTTP-1003

Message `<timestamp>, [HTTP-1003], <sequence-number>, AUDIT, INFO, <system-name>, Zoning transaction initiated by User: <User Name>, Role: <User Role> could not be completed successfully - <Reason Message>.`

Probable cause Indicates an error in completing the zoning transaction.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

41

IBD System Messages

This chapter contains information on the following IBD message:

- IBD-1001 504

IBD-1001

Message

```
<timestamp>, [FKLB-1001], <sequence-number>,, ERROR,
<system-name>, Slot <slot number>, Port GE<port number>:
Maximum attempts to restart failed. Disabling port.
```

Probable cause

Indicates that the specified port has crashed unexpectedly and restarting attempts have failed.

Recommended action

Power off and power on the blade using the **slotPowerOff** and **slotPowerOn** commands. On the MP-7500B or AP-7600B, switch off and on all primary power in order to power-cycle the unit.

Severity

WARNING

42

IBPD System Messages

This chapter contains information on the following IBPD messages:

- IBPD-1001 506
- IBPD-1002 506
- IBPD-1003 506

IBPD-1001

Message

```
<timestamp>, [IBPD-1001], <sequence-number>,, WARNING,
<system-name>, <Function name>:<Line number> initiator
name length exceeds the <Max length limit> character
limit
[<Initiator name>]
```

Probable cause Indicates that the initiator name length exceeds the supported limit of characters.

Recommended action Change the initiator name, keeping the number of characters within the supported limit.

Severity WARNING

IBPD-1002

Message

```
<timestamp>, [IBPD-1002], <sequence-number>,, WARNING,
<system-name>, <Function name>:<Line number> target name
length exceeds the <Max length limit> character limit
[<target name>]
```

Probable cause Indicates that the target name length exceeds the supported limit.

Recommended action Redo the discovery to get the latest target list, and try again.

Severity WARNING

IBPD-1003

Message

```
<timestamp>, [IBPD-1003], <sequence-number>,, WARNING,
<system-name>, iSCSI login sessions exceed the maximum
limit at slot <Slot number> port ge<Port number>
```

Probable cause Indicates that the iSCSI login sessions exceed the supported limit per port.

Recommended action Use another port to login.

Severity WARNING

43

ICPD System Messages

This chapter contains information on the following ICPD messages:

- ICPD-1001 508
- ICPD-1002 508
- ICPD-1003 508
- ICPD-1004 509
- ICPD-1005 509
- ICPD-1006 509
- ICPD-1007 510
- ICPD-1008 510

ICPD-1001

Message `<timestamp>, [ICPD-1001], <sequence-number>,, ERROR, <system-name>, Failed to allocate memory: (<function name>).`

Probable cause Indicates that the specified function failed to allocate memory.

Recommended action Check memory usage on the switch using the **memShow** command.

Reboot or power cycle the switch.

Severity ERROR

ICPD-1002

Message `<timestamp>, [ICPD-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module> rc = <error>.`

Probable cause Indicates that an initialization of a module within the ICPD failed.

Recommended action Use the **firmwareDownload** command to download a new firmware version.

Severity ERROR

ICPD-1003

Message `<timestamp>, [ICPD-1003], <sequence-number>,, INFO, <system-name>, iSCSI configuration has been committed by switch (<domain id>).`

Probable cause Indicates that iSCSI configuration has been committed by a remote switch in the fabric.

Recommended action No action is required.

Severity INFO

ICPD-1004

Message `<timestamp>, [ICPD-1004], <sequence-number>,, WARNING, <system-name>, iSNS Client service is detected on multiple switches in fabric.`

Probable cause Indicates that iSNS Client service is enabled on multiple switches in fabric.

Recommended action Enable the iSNS Client service on a single switch in the fabric using the **fosConfig** command.

Severity WARNING

ICPD-1005

Message `<timestamp>, [ICPD-1005], <sequence-number>,, WARNING, <system-name>, iSCSI configuration between local switch (<local domain id>) and peer (<peer domain id>) is out of sync. iSCSI login is not allowed.`

Probable cause Indicates that iSCSI switches in the fabric have different configurations in AUTH, VT, or DD.

Recommended action Sync up the configuration in the fabric using the **iscsiCfg** command.

Severity WARNING

ICPD-1006

Message `<timestamp>, [ICPD-1006], <sequence-number>,, INFO, <system-name>, iSCSI service is <status> on the switch.`

Probable cause Indicates that the iSCSI service is enabled or disabled on the switch.

Recommended action No action is required.

Severity INFO

ICPD-1007

Message `<timestamp>, [ICPD-1007], <sequence-number>,, INFO, <system-name>, iSNSC service is <status> on the switch.`

Probable cause Indicates that the iSNSC service is enabled or disabled on the switch.

Recommended action No action is required.

Severity INFO

ICPD-1008

Message `<timestamp>, [ICPD-1008], <sequence-number>,, INFO, <system-name>, iSCSI switch (<domain id>) is <status>.`

Probable cause Indicates that the iSCSI switch is reachable or unreachable.

Recommended action No action is required.

Severity INFO

44

IPAD System Messages

This chapter contains information on the following IPAD messages:

- IPAD-1000 512
- IPAD-1001 512

IPAD-1000

Message

```
<timestamp>, [IPAD-1000], <sequence-number>,, INFO,
<system-name> <Type of managed entity> <Instance number
of managed entity> <Type of network interface> <Instance
number of network interface> <Protocol address family>
<Source of address change> <Value of address and prefix>
<DHCP enabled or not>
```

Probable cause

Indicates that a change in local IP address has occurred. If the source of the address change is manual, this means that the address change was initiated by a user. If the source of the address change is the dynamic host configuration protocol (DHCP), this means that the address change was due to interaction with a DHCP server.

Recommended action

No action is required.

Severity

INFO

IPAD-1001

Message

```
<timestamp>, [IPAD-1001], <sequence-number>,, INFO,
<system-name> <Type of managed entity> <Instance number
of managed entity> <Protocol address family> <Source of
address change> <Value of addres> <DHCP enabled or not>
```

Probable cause

Indicates that a change in gateway IP address has occurred. If the source of the address change is manual, this means that the address change was initiated by a user. If the source of the address change is the dynamic host configuration protocol (DHCP). This means that the address change was due to interaction with a DHCP server.

Recommended action

No action is required.

Severity

INFO

45

IPS System Messages

This chapter contains information on the following IPS messages:

- IPS-1001 514
- IPS-1002 514
- IPS-1003 514
- IPS-1004 515
- IPS-1005 515
- IPS-1006 516

IPS-1001

Message

```
<timestamp>, [IPS-1001], <sequence-number>,, WARNING,
<system-name>, <message> FCIP License Not Installed
(<error>)
```

Probable cause

Indicates that the FCIP license is not installed on the switch.

Recommended action

Run the **licenseShow** command to check the installed licenses on the switch. Contact your EMC account representative for an FCIP license. Run the **licenseAdd** command to add the license to your switch.

Severity

WARNING

IPS-1002

Message

```
<timestamp>, [IPS-1002], <sequence-number>,, ERROR,
<system-name>, Failed to initialize <module> rc = <error>
```

Probable cause

Indicates that an initialization of a module within the IPS daemon failed.

Recommended action

Use the **firmwareDownload** command to download a new firmware version.

Severity

ERROR

IPS-1003

Message

```
<timestamp>, [IPS-1003], <sequence-number>,, WARNING,
<system-name>, <function name>(): Failed to allocate
memory while performing <message>
```

Probable cause

Indicates that memory resources are low. This might be a transient problem.

Recommended action

If the message persists, check the memory usage on the switch, using the **memShow** command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

IPS-1004

Message

```
<timestamp>, [IPS-1004], <sequence-number>,, WARNING,
<system-name>, Port Config Mode Mismatch slot (<slot>)
port(ge<port>): current mode is (<current mode>)
```

Probable cause Indicates that configured Port Mode is different from intended use.

Recommended action Change the port configuration (by deleting configured FCIP tunnels or iSCSI sessions) to return the port mode to neutral before attempting to configure the port for a different mode or use.

Severity WARNING

IPS-1005

Message

```
<timestamp>, [IPS-1005], <sequence-number>,, WARNING,
<system-name>, Tunnel Authorization Failure for slot
(<slot>) port(ge<port>) tunnel ID(<tunnel number>) reason
(<reason>)
```

Probable cause Indicates that tunnel setup failed due to authorization failure from the remote side. Reasons for such failures could be a WWN Mismatch.

Recommended action Change the tunnel configuration on one side of the tunnel to authorize remote side to setup tunnel.

Severity WARNING

IPS-1006

Message

```
<timestamp>, [IPS-1006], <sequence-number>,, WARNING,
<system-name>, Tunnel Configuration Mismatch for slot
(<slot>) port(<port>) tunnel ID(<tunnel number>) reason
(<reason>)
```

Probable cause

Indicates that tunnel setup failed due to a configuration mismatch between the two ends. Reasons for such a mismatch could be the Compression, SACK, FastWrite, and TapePipelining setting.

Recommended action

Change the tunnel configuration on one side of the tunnel to match that of the other side to setup tunnel.

Severity

WARNING

46

ISCS System Messages

This chapter contains information on the following ISCS message:

- ISCS-1000 518

ISCS-1000

Message `<timestamp>, [ISCS-1000], <sequence-number>,, ERROR, <system-name>, Slot <slot number> Port GE<port number> crashed unexpectedly.`

Probable cause Indicates that specified port has crashed.

Recommended action No action is required; the port will restart automatically.

Severity ERROR

47

ISNS System Messages

This chapter contains information on the following ISNS messages:

- ISNS-1001 520
- ISNS-1002 520
- ISNS-1003 520
- ISNS-1004 521
- ISNS-1005 521
- ISNS-1006 521
- ISNS-1008 522
- ISNS-1009 522
- ISNS-1010 522
- ISNS-1011 523
- ISNS-1013 523
- ISNS-1014 523

ISNS-1001

Message `<timestamp>, [ISNS-1001], <sequence-number>,, INFO, <system-name>, Configuration peering with external iSNS server <New config iSNS server IP address> slot/port <New config Slot number>/ge<New config port number> (current <Current iSNS server IP address> <Current slot number>/ge<Current port number>).`

Probable cause Indicates that the user has issued the **isnscCfg** command.

Recommended action No action is required.

Severity INFO

ISNS-1002

Message `<timestamp>, [ISNS-1002], <sequence-number>,, INFO, <system-name>, Start peering with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Probable cause Indicates that peering has started with the specified external internet storage name service (iSNS) server.

Recommended action No action is required.

Severity INFO

ISNS-1003

Message `<timestamp>, [ISNS-1003], <sequence-number>,, INFO, <system-name>, Peering with external iSNS server is disabled.`

Probable cause Indicates that the IP address of internet storage name service (iSNS) server is set to zero, so peering is disabled.

Recommended action If you wish to enable the iSNS server, use the **isnscCfg** command to show or set the server IP address; otherwise, no action is required.

Severity INFO

ISNS-1004

Message

```
<timestamp>, [ISNS-1004], <sequence-number>,, WARNING,
<system-name>, Timeout refreshing iSNS database with iSNS
server <iSNS server IP address> slot/port <Slot
number>/ge<Port number> Reg-Period <Registration-Period
in seconds>.
```

Probable cause Indicates that the internet storage name service (iSNS) client failed to receive a successful response for a DevAttrQry within the specified *Registration-Period*.

Recommended action Verify the connection of the iSNS server to the slot/port.

Severity WARNING

ISNS-1005

Message

```
<timestamp>, [ISNS-1005], <sequence-number>,, INFO,
<system-name>, User request re-register with external
iSNS server <iSNS server IP address> slot/port <Slot
number>/ge<Port number>.
```

Probable cause Indicates that the user has requested a re-register with the specified external internet storage name service (iSNS) server.

Recommended action No action is required.

Severity INFO

ISNS-1006

Message

```
<timestamp>, [ISNS-1006], <sequence-number>,, INFO,
<system-name>, Start re-register with external iSNS
server <iSNS server IP address> slot/port <Slot
number>/ge<Port number>.
```

Probable cause Indicates that the re-register with the specified external internet storage name service (iSNS) server has started.

Recommended action No action is required.

Severity INFO

ISNS-1008

Message `<timestamp>, [ISNS-1008], <sequence-number>,, INFO, <system-name>, Peering with external iSNS server <iSNS server IP address> not started because configuration unchanged.`

Probable cause Indicates that peering with the external iSNS server was already started with the same configuration.

Recommended action No action is required. You may change the configuration and retry the peering with the external iSNS server.

Severity INFO

ISNS-1009

Message `<timestamp>, [ISNS-1009], <sequence-number>,, INFO, <system-name>, Peering with external iSNS server <iSNS server IP address>not started because no virtual targets found.`

Probable cause Indicates that no virtual targets were found, so peering was not started.

Recommended action No action is required. Peering will resume automatically when virtual targets are detected.

Severity INFO

ISNS-1010

Message `<timestamp>, [ISNS-1010], <sequence-number>,, WARNING, <system-name>, Slot/port <Slot>/ge<Port> is out of range.`

Probable cause Indicates that the slot or port is out of range.

Recommended action Retry with a valid slot/port. Refer to the appropriate hardware reference manual for valid slot and port ranges.

Severity WARNING

ISNS-1011

Message

```
<timestamp>, [ISNS-1011], <sequence-number>,, INFO,
<system-name>, iSNS Client Service is <iSNS client State
(enabled/disabled)>.
```

Probable cause Indicates the current state of the internet storage name service (iSNS) Client as enabled or disabled.

Recommended action No action is required. Use the **fosConfig** command to display, enable, or disable the iSNS Client service.

Severity INFO

ISNS-1013

Message

```
<timestamp>, [ISNS-1013], <sequence-number>,, WARNING,
<system-name>, iSNS server connection failure.
```

Probable cause Indicates that the internet storage name service (iSNS) client failed to establish a connection with the iSNS server.

Recommended action Verify the connection of the iSNS server to the slot/port. Use the isnscCfg command to display or correct the server IP address.

Severity WARNING

ISNS-1014

Message

```
<timestamp>, [ISNS-1014], <sequence-number>,, INFO,
<system-name>, Start peering with external iSNS server
<iSNS server IP address> on management port.
```

Probable cause Indicates that peering has started with the specified external internet storage name service (iSNS) on the management port.

Recommended action No action is required.

Severity INFO

48

KAC System Messages

This chapter contains information on the following KAC messages:

- KAC-1002 526
- KAC-1004 526
- KAC-1006 526
- KAC-1007 527
- KAC-1008 527

KAC-1002

Message `<timestamp>, [KAC-1002], <sequence-number>,, ERROR, <system-name>, KAC(<Key Vault Type>) communication Error: Error connecting to <Backup or Primary>.`

Probable Cause Indicates that the key archival client is unable to communicate with the *primary* or *backup* key vault.

Recommended Action Determine whether the configured key value is operational, and if it is not, change the switch key vault settings.

Severity ERROR

KAC-1004

Message `<timestamp>, [KAC-1004], <sequence-number>,, ERROR, <system-name>, KAC <Operation Description> to key vault failed.`

Probable Cause Indicates that the key archival client is unable to do a certain operation to the *primary* or *backup* key vault.

Recommended Action Determine whether the configured key value is operational, and if it is not, change the switch key vault settings.

Severity ERROR

KAC-1006

Message `<timestamp>, [KAC-1006], <sequence-number>,, ERROR, <system-name>, Switch to key vault trustee link was not established.`

Probable Cause Indicates that the link from the switch to the key vault trustee was not established.

Recommended Action Establish a trustee link between the switch and the key vault.

Severity ERROR

KAC-1007

Message

```
<timestamp>, [KAC-1007], <sequence-number>,, ERROR,
<system-name>, KAC put key to key vault failed, LUN=<LUN
Number>, keyID=<Key ID Value>, errno=<Error Number>.
```

Probable Cause

Indicates that the key archival client is unable to put to the *primary* or *backup* key vault.

Recommended Action

Determine whether the configured key value is operational, and if it is not, change the switch key vault settings.

Severity

ERROR

KAC-1008

Message

```
<timestamp>, [KAC-1008], <sequence-number>,, ERROR,
<system-name>, Putting TEP failed check if there is
already an unapproved TEP then delete it, RC=<Error code
from lkm>.
```

Probable Cause

Indicates that there was already a pending unapproved Trusted Establishment Package (TEP) at the LifeTime Key Management Appliance (LKM).

Recommended Action

Log in to the LKM and delete the unapproved TEP.

Severity

ERROR

49

KSWD System Messages

This chapter contains information on the following KSWD message:

- KSWD-1001 530
- KSWD-1002 530
- KSWD-1003 530

KSWD-1001

Message

<timestamp>, [KSWD-1001], <sequence-number>, FFDC, WARNING, <system-name>, <Software component>:<Software component Process ID> failed to refresh (<Current time>:<Refresh time>).

Probable Cause

Indicates one of the critical daemons is found to be nonresponsive. An abort signal is sent.

Recommended Action

Run supportFtp (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

KSWD-1002

Message

<timestamp>, [KSWD-1002], <sequence-number>, FFDC, WARNING, <system-name>, Detected termination of process <Software component>:<Software component Process ID>.

Probable Cause

Indicates a process on the switch has ended unexpectedly.

Recommended Action

Run supportFtp (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

KSWD-1003

Message

<timestamp>, [KSWD-1003], <sequence-number>, FFDC, WARNING, <system-name>, kSWD: <Warning message>.

Probable Cause

Indicates a warning state within the system.

A critical application error was reported in the watchdog subsystem. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or fail over (on dual-CP switches).

The *warning message* will be one of the following:

- <Detected unexpected termination of: <daemon name>>

  Probable Cause: One of the critical daemons ended unexpectedly.

- <<daemon name> failed to refresh SWD*** Sending SIGABRT to pid <process id number>>

  Probable Cause: One of the critical daemons is found to be nonresponsive; sending signal abort.

Recommended Action

SIGABRT is the signal thrown by the programs to abort the process.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

50

KTRC System Messages

This chapter contains information on the following KTRC messages:

- KTRC-1001 534
- KTRC-1002 534
- KTRC-1003 534
- KTRC-1004 535
- KTRC-1005 535

KTRC-1001

Message `<timestamp>, [KTRC-1001], <sequence-number>,, WARNING, <system-name>, Dump memory size exceeds dump file size`

Probable cause Indicates that the dump memory size has exceeded the dump file size.

Recommended action No action is required.

Severity WARNING

KTRC-1002

Message `<timestamp>, [KTRC-1002], <sequence-number>,, INFO, <system-name>, Concurrent trace dumping.`

Probable cause Indicates that the initial background dump has not completed.

Recommended action No action is required.

Severity INFO

KTRC-1003

Message `<timestamp>, [KTRC-1003], <sequence-number>,, ERROR, <system-name>, Cannot open ATA dump device`

Probable cause Indicates that the ATA dump driver is not initialized properly.

Recommended action No action is required.

Severity ERROR

KTRC-1004

Message `<timestamp>, [KTRC-1004], <sequence-number>,, ERROR, <system-name>, Cannot write to ATA dump device`

Probable cause Indicates that the write boundry in the ATA dump device has been exceeded.

Recommended action No action is required.

Severity ERROR

KTRC-1005

Message `<timestamp>, [KTRC-1005], <sequence-number>,, ERROR, <system-name>, Trace initialization failed. <Reason initialization failed>. <Internal error code>.`

Probable cause Indicates that Trace was unable to initialize.

Recommended action No action is required.

Severity ERROR

51

LFM System Messages

This chapter contains information on the following LOG messages:

- LFM-1001 538
- LFM-1002 538
- LFM-1003 538
- LFM-1004 539
- LFM-1005 539
- LFM-1006 539

LFM-1001

Message `<timestamp>, [LFM-1001], <sequence-number>,, INFO, <system-name>, The Logical Fabric Manager service is disabled.`

Probable Cause Indicates that the Logical Fabric Manager service is disabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user configurable.

Recommended Action No action is required.

Severity INFO

LFM-1002

Message `<timestamp>, [LFM-1002], <sequence-number>,, INFO, <system-name>, The Logical Fabric Manager service is enabled.`

Probable Cause Indicates that the Logical Fabric Manager service is enabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user configurable.

Recommended Action No action is required.

Severity INFO

LFM-1003

Message `<timestamp>, [LFM-1003], <sequence-number>,, INFO, <system-name>, The Logical Fabric Manager configuration is set to default.`

Probable Cause Indicates that the Logical Fabric Manager configuration is set to default. This will remove all prior Logical Fabric Manager configurations. This operation is currently not supported.

Recommended Action No action is required.

Severity INFO

LFM-1004

Message
```
<timestamp>, [LFM-1004], <sequence-number>,, CRITICAL,
<system-name>, HA is out of sync for opcode <HA OPCODE>,
error value <error value>.
```

Probable Cause Indicates the trigger for some internal logging purposes.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity CRITICAL

LFM-1005

Message
```
<timestamp>, [LFM-1005], <sequence-number>,, WARNING,
<system-name>, Logical port <portnum> disabled with
reason <portnum>(<reason>).
```

Probable Cause Indicates a Logical ISL (LISL) was disabled due to protocol conflict or security/policy violation. This can result in possible traffic issues.

Recommended Action Check the reason for port disable using the **switchshow** command, rectify the cause and re-enable the LISL using the **lfcfg --lislenable** command.

Severity CRITICAL

LFM-1006

Message
```
<timestamp>, [LFM-1006], <sequence-number>,, WARNING,
<system-name>, The switch with domain <domain> with
firmware version <version> has joined the FID <FID>
fabric and may not be compatible with XISL use.
```

Probable Cause Indicates that the validation for firmware compatibility of the specified switch for Extended ISL (XISL) use failed.

Recommended Action Check release notes to verify the firmware version is compatible with XISL use. If it is not, run the **firmwareDownload** command to upgrade the firmware, or remove the switch from the fabric.

Severity WARNING

52

LOG System Messages

This chapter contains information on the following LOG messages:

- LOG-1000 542
- LOG-1001 542
- LOG-1002 543
- LOG-1003 543

LOG-1000

Message

```
<timestamp>, [LOG-1000], <sequence-number>,, INFO,
<system-name>, Previous message repeated <repeat count>
time(s)
```

Probable cause

Indicates that the previous message repeated the specified number of times.

Recommended action

No action is required.

Severity

INFO

LOG-1001

Message

```
<timestamp>, [LOG-1001], <sequence-number>, FFDC,
WARNING, <system-name>, A log message was dropped
```

Probable cause

Indicates that a log message was dropped. A trace dump file is created.

Recommended action

Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

LOG-1002

Message

```
<timestamp>, [LOG-1002], <sequence-number>, FFDC,
WARNING, <system-name>, A log message was dropped
```

Probable cause

Indicates that a message was not recorded by the error logging system. A trace dump file is created. The message might still be visible through SNMP or other management tools.

Recommended action

Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

LOG-1003

Message

```
<timestamp>, [LOG-1003], <sequence-number>,, INFO,
<system-name>, The log has been cleared.
```

Probable cause

Indicates that the persistent error log has been cleared.

Recommended action

No action is required.

Severity

INFO

53

LSDB System Messages

This chapter contains information on the following LSDB messages:

- LSDB-1001 546
- LSDB-1002 546
- LSDB-1003 547
- LSDB-1004 547

LSDB-1001

Message

```
<timestamp>, [LSDB-1001], <sequence-number>,, ERROR,
<system-name>, Link State ID <link state ID> out of range
```

Probable cause

Indicates that the specified link state database ID is out of the acceptable range. The valid *link state ID* is the same as the valid domain ID, whose range is from 1 through 239. The switch will discard the record because it is not supported.

Recommended action

No action is required.

Severity

ERROR

LSDB-1002

Message

```
<timestamp>, [LSDB-1002], <sequence-number>,, INFO,
<system-name>, Local Link State Record reached max
incarnation#
```

Probable cause

Indicates that the local link state database reached the maximum incarnations.

An "incarnation" is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled.

The incarnation number will begin again at 0x80000001 after reaching 0x7FFFFFFF.

Recommended action

No action is required.

Severity

INFO

LSDB-1003

Message

```
<timestamp>, [LSDB-1003], <sequence-number>, FFDC,
CRITICAL, <system-name>, No database entry for local Link
State Record, domain <local domain>
```

Probable cause

Indicates that there is no local link state record entry in the link state database. The switch should always generate its own local entry when starting up.

An "incarnation" is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled. By disabling and enabling the switch, a new local link state record is generated.

Recommended action

Run the **switchDisable** and **switchEnable** commands. A new local link state record is generated during the switch enable.

Severity

CRITICAL

LSDB-1004

Message

```
<timestamp>, [LSDB-1004], <sequence-number>,, WARNING,
<system-name>, No Link State Record for domain <local
domain>
```

Probable cause

Indicates that there is no link state record for the specified *local domain*.

Recommended action

No action is required. The other switch will pass the LSD when the fabric has become stable.

Severity

WARNING

54

MFIC System Messages

This chapter contains information on the following MFIC messages:

- MFIC-1001 550
- MFIC-1002 550
- MFIC-1003 551

MFIC-1001

Message

```
<timestamp>, [MFIC-1001], <sequence-number>,, ERROR,
<system-name>, failure at sysmod_scn registry rc=
<failure reason>
```

Probable cause

Indicates that the system is temporarily out of resources.

Recommended action

No action is required; this message is often transitory.

If the message persists, run a switch **reboot** or an **haFailover** (if applicable).

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

MFIC-1002

Message

```
<timestamp>, [MFIC-1002], <sequence-number>,, INFO,
<system-name>, Chassis FRU header not programmed for
switch NID, using defaults (applies only to FICON
environments).
```

Probable cause

Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR).

The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended action

No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

Severity

INFO

MFIC-1003

Message

```
<timestamp>, [MFIC-1003], <sequence-number>,, WARNING,
<system-name>, Effective Insistent domain ID for the
fabric changed from <state> to <state>
```

Probable cause

Indicates that one or more switches joined the fabric with a different insistent domain ID (IDID) mode setting than the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for *state* are "On" or "Off".

Recommended action

IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required.

IDID mode can be set using the **configure** command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure Tab > Fabric Subtab > Insistent Domain ID Mode** checkbox. The switch must be disabled to change the IDID mode.

Severity

WARNING

55

MPTH System Messages

This chapter contains information on the following MPTH messages:

- MPTH-1001 554
- MPTH-1002 554
- MPTH-1003 554

MPTH-1001

Message `<timestamp>, [MPTH-1001], <sequence-number>, FFDC, ERROR, <system-name>, Null parent, lsId = <number>`

Probable cause Indicates that a null parent was reported. MPATH uses a tree structure in which the parent is used to connect to the root of the tree.

Recommended action No action is required.

Severity ERROR

MPTH-1002

Message `<timestamp>, [MPTH-1002], <sequence-number>, FFDC, ERROR, <system-name>, Null lsrP, lsId = <ls ID number>`

Probable cause Indicates that a link state record is null.

Recommended action No action is required.

Severity ERROR

MPTH-1003

Message `<timestamp>, [MPTH-1003], <sequence-number>,, WARNING, <system-name>, No minimum cost path in candidate list`

Probable cause Indicates that the FSPF module has determined that there is no minimum cost path (MPath) available in the candidate list.

Recommended action No action is required.

Severity WARNING

56

MQ System Messages

This chapter contains information on the following MQ message.

- MQ-1004 556

MQ-1004

Message

```
<timestamp>, [MQ-1004], <sequence-number>,, ERROR,
<system-name>, mqRead, queue = <queue name>, queue ID =
<queue ID>, type = <message type>
```

Probable cause

Indicates that an unexpected message has been received in the specified message queue. The *queue name* is always fspf_q. The *queue ID* and corresponding *message type* can be any of the following:

- 2 - MSG_TX
- 3 - MSG_INTR
- 4 - MSG_STR
- 6 - MSG_ASYNC_IU
- 7 - MSG_LINIT_IU
- 8 - MSG_RSCN
- 9 - MSG_IOCTL
- 10 - MSG_ACCEPT
- 11 - MSG_IU_FREE
- 12 - MSG_US
- 13 - MSG_EXT_RSCN
- 14 - MSG_RDTS_START
- 15 - MSG_RDTS_SENDEFP
- 16 - MSG_RDTS_RESET

Recommended action

No action is required.

Severity

ERROR

57

MS System Messages

This chapter contains information on the following MS messages:

- MS-1001 558
- MS-1002 558
- MS-1003 559
- MS-1004 560
- MS-1005 560
- MS-1006 561
- MS-1008 561
- MS-1009 562
- MS-1021 562
- MS-1022 563
- MS-1023 563
- MS-1024 563

MS-1001

Message

```
<timestamp>, [MS-1001], <sequence-number>,, WARNING,
<system-name>, MS Platform Segmented port=<port
number>(<reason for segmentation> <domain>)
```

Probable cause

Indicates that the management server (MS) has segmented from another switch *domain* at the specified *port number* due to errors or inconsistencies defined in the MS platform service.

Recommended action

Reboot or power cycle the switch.

Severity

WARNING

MS-1002

Message

```
<timestamp>, [MS-1002], <sequence-number>,, INFO,
<system-name>, MS Platform Service Unstable(<message
string><domain number>)
```

Probable cause

The management server (MS) platform service is unstable.

The *message string* can be one of the following:

- <No Resp for GCAP from>
  The switch did not respond to a request for GCAP (MS Get Capabilities) command.

  Recommended action: No action is required.
- <GCAP sup but not PL by>
  The GCAP (MS Get Capabilities) is supported but the flag for MS platform service is not set.

  Recommended action: Set the flag for the MS Platform Service.
- <GCAP Rejected (reason =BUSY) by>
  The GCAP (MS Get Capabilities) is not supported by another switch.

  Recommended action: Run the **firmwareDownload** command to upgrade the firmware level on the switch to a level that supports RCS.

- <Reject EXGPLDB from>
  The request to the exchange platform database was rejected. The remote switch might be busy.

  Recommended action: Wait a few minutes and try the command again.

The *domain number* is the target domain that caused error.

Recommended action

The recommended actions are as follows:

- <No Resp for GCAP from>
  No action is required.
- <GCAP sup but not PL by>
  Set the flag for the MS Platform Service.
- <GCAP Rejected (reason =BUSY) by>
  Run the **firmwareDownload** command to upgrade the firmware level on the switch to a level that supports RCS. RCS is supported in Fabric OS v2.6, v3.1 and greater, and v4.1 and greater.
- <Reject EXGPLDB from>
  Wait a few minutes and try the command again.

Severity

INFO

MS-1003

Message

```
<timestamp>, [MS-1003], <sequence-number>,, INFO,
<system-name>, MS detected Unstable Fabric(<message
string><domain number>).
```

Probable cause

Indicates that the management server (MS) detected an unstable fabric; the command or operation might not be successfully completed. This message is often transitory.

The *message string* can be one of the following:

- <DOMAIN_INVALID for a req from>
  The domain is invalid for a request.
- <No WWN for>
  Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain number* is the target domain that caused error.

Recommended action

The fabric might be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

INFO

MS-1004

Message

```
<timestamp>, [MS-1004], <sequence-number>,, INFO,
<system-name>, MS detected ONLY 1 Domain(d=<domain in
local resource>).
```

Probable cause

Indicates that the management server (MS) detected an unstable count of domains in its own local resource.

Recommended action

This message is often transitory.

The fabric might be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

INFO

MS-1005

Message

```
<timestamp>, [MS-1005], <sequence-number>,, ERROR,
<system-name>, MS Invalid CT Response from d=<domain>
```

Probable cause

Indicates that the management server (MS) received an invalid common transport (CT) response from switch *domain*. MS expects either a CT accept IU or a reject IU; MS received neither response,

which violates the Fibre Channel Generic Services (FS-GS) specification.

Recommended action Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the FC-FS standard.

Severity ERROR

MS-1006

Message

```
<timestamp>, [MS-1006], <sequence-number>,, ERROR,
<system-name>, MS Unexpected iu_data_sz=<number of bytes>
```

Probable cause Indicates that management server (MS) received information unit (IU) data of unexpected size. The IU payload and the IU size might be inconsistent with each other or with the command that is currently being processed.

Recommended action Wait a few minutes and try the operation again.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

MS-1008

Message

```
<timestamp>, [MS-1008], <sequence-number>,, ERROR,
<system-name>, MS Failure while initializing <action>
```

Probable cause The management server (MS) failed while initializing the specified *action*.

The following *actions* might be displayed:

- <while writing to ms_els_q>
  MS is unable to write a message to the MS Extended Link Service Queue.
- <while inserting timer to timer list>
  MS is unable to add a timer to a resource.

Recommended action This message is often transitory.

If the message persists, check the available memory on the switch using **memShow**.

Severity ERROR

MS-1009

Message

```
<timestamp>, [MS-1009], <sequence-number>,, ERROR,
<system-name>, RLIR event. Switch Port ID is <PID>.
Device Port Tag is <port tag>. <message>.
```

Probable cause A Registered Link Incident Record (RLIR) has been generated for one of the actions clarified by the <message> passed in.

The following *messages* might be displayed:

- Exceeded bit error rate threshold
- Loss of signal or synchronization
- Not operational seq. recognized
- Primitive sequence timeout
- Unrecognized link incident

Recommended action Persistent RLIR incidents are likely due to SAN hardware problems such as bad cables, small form-factor pluggables (SFPs), etc. It may be necessary to replace hardware if these messages persist.

Severity ERROR

MS-1021

Message

```
<timestamp>, [MS-1021], <sequence-number>,, ERROR,
<system-name>, MS WARMBOOT failure(FSS_MS_WARMINIT
failed. Reason=<failure reason>)
```

Probable cause Indicates that the Fabric OS state synchronization (FSS) warm recovery failed during WARM INIT phase of a reboot.

Recommended action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

MS-1022

Message `<timestamp>, [MS-1022], <sequence-number>,, INFO, <system-name>, Management Server Platform Service <Activated or Deactivated>`

Probable cause Indicates that Management Server Platform Service is being activated or deactivated.

Recommended action No action is required.

Severity INFO

MS-1023

Message `<timestamp>, [MS-1023], <sequence-number>,, INFO, <system-name>, Management Server Topology Discovery Service <Enabled or Disabled>`

Probable cause Indicates that Management Server Topology Discovery Service is being enabled or disabled.

Recommended action No action is required.

Severity INFO

MS-1024

Message `<timestamp>, [MS-1024], <sequence-number>,, INFO, <system-name>, Management Server Access Control List is Updated`

Probable cause Indicates that the management server (MS) Access Control List is saved to non-volatile storage.

Recommended action No action is required.

Severity INFO

58

NBFS System Messages

This chapter contains information on the following NBFS messages:

- NBFS-1001 566
- NBFS-1002 566
- NBFS-1003 567

NBFS-1001

Message

```
<timestamp>, [NBFS-1001], <sequence-number>,, INFO,
<system-name>, Duplicate E_Port SCN from port
<portnumber> in state <state change name> (<state change
number>)
```

Probable cause

Indicates that a duplicate E_Port State Change Number was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended action

No action is required.

Severity

INFO

NBFS-1002

Message

```
<timestamp>, [NBFS-1002], <sequence-number>, FFDC, ERROR,
<system-name>, Wrong input: <state name> to neighbor FSM,
state <current state name>, port <portnumber>
```

Probable cause

Indicates that the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, it means the protocol implementation between two connected switches has problems.

Recommended action Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is FULL, then this message can safely be ignored. Otherwise, run the **portDisable** and **portEnable** commands to refresh the port.

Severity ERROR

NBFS-1003

Message

```
<timestamp>, [NBFS-1003], <sequence-number>,, WARNING,
<system-name>, DB_XMIT_SET flag not set in state <current
state name>, input <state name>, port <portnumber>
```

Probable cause Indicates that the database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended action No action is required. The Fabric OS auto recovers from this problem.

Severity WARNING

59

NS System Messages

This chapter contains information on the following NS messages:

- NS-1001 570
- NS-1002 570
- NS-1003 571
- NS-1004 571
- NS-1005 572
- NS-1006 572

NS-1001

Message

```
<timestamp>, [NS-1001], <sequence-number>,, WARNING,
<system-name>, The response for request 0x<CT command
code> from remote switch 0x<Domain Id> is larger than the
max frame size the remote switch can support!
```

Probable cause

Indicates that the response payload exceeds the maximum frame size that the remote switch can handle.

Recommended action

Run the **firmwareDownload** command to upgrade the remote switch with firmware v4.3 or higher, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

Severity

WARNING

NS-1002

Message

```
<timestamp>, [NS-1002], <sequence-number>,, WARNING,
<system-name>, Remote switch 0x<Domain Id> has firmware
revision lower than 2.2: <Firmware Revision 1st
character><Firmware Revision 2nd character><Firmware
Revision 3rd character><Firmware Revision 4th character>
which is not supported!
```

Probable cause

Indicates that the local switch cannot interact with the remote switch due to incompatible or obsolete firmware.

Recommended action

Run the **firmwareDownload** command to upgrade the remote switch to the latest level of firmware.

Severity

WARNING

NS-1003

Message

```
<timestamp>, [NS-1003], <sequence-number>,, INFO,
<system-name>, Number of local devices <Current local
device count>, exceeds the standby can support <Local
device count that standby can support>, can't send
update.
```

Probable cause

Indicates that the name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended action

To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

Severity

INFO

NS-1004

Message

```
<timestamp>, [NS-1004], <sequence-number>,, INFO,
<system-name>, Number of local devices <Current local
device count>, exceeds the standby can support <Local
device count that standby can support>, can't sync.
```

Probable cause

Indicates that the name server on the standby CP has lower supported capability than the active CP due to different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended action

To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version. Reduce the local device count to follow the capability of the lowest version of firmware.

Severity

INFO

NS-1005

Message

```
<timestamp>, [NS-1005], <sequence-number>,, WARNING,
<system-name>, Zone size of <Effective Zone Size> has
over the supporting limit of <Support Zone Size> for the
remote switch domain ID <Remote Switch Domain ID>.
```

Probable cause Indicates that the effective zone size has exceeded the limit that a remote switch can support. The oversized portion will be truncated.

Recommended action Reduce the zone size to 1024 or less, or upgrade the software of the remote switch to support 2048 zones.

Severity WARNING

NS-1006

Message

```
<timestamp>, [NS-1006], <sequence-number>,, WARNING,
<system-name>, Duplicated WWN was detected with PID
<existing device PID> and <new device PID>.
```

Probable Cause Indicates that an existing device has the same WWN as a new device that has come online.

Recommended Action The switch will process the new PID and leave the existing PID intact. Subsequent switch operations will clean up the obsolete PID, however, administrators could check and remove devices with duplicated WWN.

Severity WARNING

60

PDM System Messages

This chapter contains information on the following PDM messages:

- PDM-1001 574
- PDM-1002 574
- PDM-1003 574
- PDM-1004 575
- PDM-1005 575
- PDM-1006 575
- PDM-1007 576
- PDM-1008 576
- PDM-1009 577
- PDM-1010 577
- PDM-1011 577
- PDM-1012 578
- PDM-1013 578
- PDM-1014 578
- PDM-1017 579
- PDM-1019 579
- PDM-1020 580
- PDM-1021 580
- PDM-1022 580
- PDM-1023 581
- PDM-1024 581

PDM-1001

Message

```
<timestamp>, [PDM-1001], <sequence-number>,, WARNING,
<system-name>, Failed to parse the pdm config.
```

Probable cause

Indicates that the parity data manager (PDM) process could not parse the configuration file. This might be caused by a missing configuration file during the installation.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

PDM-1002

Message

```
<timestamp>, [PDM-1002], <sequence-number>,, WARNING,
<system-name>, ipcInit failed.
```

Probable cause

Indicates that the parity data manager (PDM) process could not initialize the inter-process communication (IPC) mechanism.

Recommended action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

PDM-1003

Message

```
<timestamp>, [PDM-1003], <sequence-number>,, WARNING,
<system-name>, pdm [-d] -S <service> -s <instance>.
```

Probable cause

Indicates that a syntax error occurred when trying to launch the parity data manager (PDM) process.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1004

Message

```
<timestamp>, [PDM-1004], <sequence-number>,, WARNING,
<system-name>, PDM memory shortage.
```

Probable cause Indicates that the parity data manager (PDM) process ran out of memory.

Recommended action Reboot or power cycle the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1005

Message

```
<timestamp>, [PDM-1005], <sequence-number>,, WARNING,
<system-name>, FSS register failed.
```

Probable cause Indicates that the parity data manager (PDM) failed to register with the Fabos synchronization service (FSS).

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1006

Message

```
<timestamp>, [PDM-1006], <sequence-number>,, WARNING,
<system-name>, Too many files in sync.conf.
```

Probable cause Indicates that the configuration file *sync.conf* contains too many entries.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1007

Message

```
<timestamp>, [PDM-1007], <sequence-number>,, WARNING,
<system-name>, File not created: <file name>.
```

Probable cause Indicates that the parity data manager (PDM) process failed to create the specified file.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1008

Message

```
<timestamp>, [PDM-1008], <sequence-number>,, WARNING,
<system-name>, Failed to get the number of U_Ports.
```

Probable cause Indicates that the parity data manager (PDM) system call to **getCfg** failed.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1009

Message

```
<timestamp>, [PDM-1009], <sequence-number>,, WARNING,
<system-name>, Can't update Port Config Data.
```

Probable cause

Indicates that the parity data manager (PDM) system call to **setCfg** failed.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

PDM-1010

Message

```
<timestamp>, [PDM-1010], <sequence-number>,, WARNING,
<system-name>, File open failed: <file name>
```

Probable cause

Indicates that the parity data manager (PDM) process could not open the specified file.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

PDM-1011

Message

```
<timestamp>, [PDM-1011], <sequence-number>,, WARNING,
<system-name>, File read failed: <file name>
```

Probable cause

Indicates that the parity data manager (PDM) process could not read data from the specified file.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1012

Message

```
<timestamp>, [PDM-1012], <sequence-number>,, WARNING,
<system-name>, File write failed: <file name>
```

Probable cause Indicates that the parity data manager (PDM) process could not write data to the specified file.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1013

Message

```
<timestamp>, [PDM-1013], <sequence-number>,, WARNING,
<system-name>, File empty: <File Name>
```

Probable cause Indicates that the switch configuration file */etc/fabos/fabos.[0|1].conf* is empty.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1014

Message

```
<timestamp>, [PDM-1014], <sequence-number>,, WARNING,
<system-name>, Access sysmod failed.
```

Probable cause Indicates that a system call to **sysMod** failed.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1017

Message

```
<timestamp>, [PDM-1017], <sequence-number>, FFDC,
CRITICAL, <system-name>, System (<Error Code>):
<Command>.
```

Probable cause Indicates that the specified system call failed.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity CRITICAL

PDM-1019

Message

```
<timestamp>, [PDM-1019], <sequence-number>,, WARNING,
<system-name>, File path or trigger too long.
```

Probable cause Indicates that one line of the *pdm.conf* file is too long.

Recommended action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

PDM-1020

Message

```
<timestamp>, [PDM-1020], <sequence-number>,, WARNING,
<system-name>, Long path name (<Path>/<File Name>), Skip.
```

Probable cause

Indicates that the indicated file path name is too long. The maximum character limit is 49 characters.

Recommended action

Use path names not exceeding 49 characters in length for the files to be replicated.

Severity

WARNING

PDM-1021

Message

```
<timestamp>, [PDM-1021], <sequence-number>,, WARNING,
<system-name>, Failed to download area port map.
```

Probable cause

Indicates that a system call failed.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

PDM-1022

Message

```
<timestamp>, [PDM-1022], <sequence-number>,, WARNING,
<system-name>, The switch is configured only with IPv6.
```

Probable cause

Indicates that the parity data manager (PDM) cannot sync with its peer because the firmware does not support IPv6.

Recommended action

Configure the local switch with IPv4 addresses.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

PDM-1023

Message

```
<timestamp>, [PDM-1023], <sequence-number>,, WARNING,
<system-name>, Radius is configured for IPv6.
```

Probable cause

Indicates that the parity data manager (PDM) cannot sync with its peer because the Radius server is configured for IPv6 addresses. IPv6 is not supported by older firmware.

Recommended action

Configure the Radius with IPv4 addresses.

Severity

WARNING

PDM-1024

Message

```
<timestamp>, [PDM-1021], <sequence-number>,, WARNING,
<system-name>, DNS is configured for IPv6.
```

Probable cause

Indicates that the parity data manager (PDM) cannot sync with its peer because the domain name service (DNS) is configured for IPv6. IPv6 is not supported by older firmware.

Recommended action

Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

61

PDTR System Messages

This chapter contains information on the following PDTR messages:

- PDTR-1001 584
- PDTR-1002 584

PDTR-1001

Message

```
<timestamp>, [PDTR-1001], <sequence-number>,, INFO,
<system-name>, < informational message >
```

Probable cause

Indicates that information has been written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

Recommended action

Run the **pdShow** command to view the panic dump and core dump files.

Severity

INFO

PDTR-1002

Message

```
<timestamp>, [PDTR-1002], <sequence-number>,, INFO,
<system-name>, < informational message >
```

Probable cause

This message indicates that information has been written to the panic dump and core dump files and a trap generated. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

Recommended action

Run the **pdShow** command to view the panic dump and core dump files.

Severity

INFO

62

PLAT System Messages

This chapter contains information on the following PLAT messages:

- PLAT-1000 586
- PLAT-1001 586
- PLAT-1002 587
- PLAT-1003 587

PLAT-1000

Message

```
<timestamp>, [PLAT-1000], <sequence-number>, FFDC,
CRITICAL, <system-name>, <Function name> <Error string>
```

Probable cause

Indicates that nonrecoverable PCI errors have been detected.

Recommended action

The system will be faulted and might automatically reboot.

If the system does not reboot, then try issuing the **reboot** command from a command-line prompt.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

PLAT-1001

Message

```
<timestamp>, [PLAT-1001], <sequence-number>,, INFO,
<system-name>, CP <Identifies which CP (0 or 1> is doing
the reset> resetting other CP (double reset may occur).
```

Probable cause

Indicates that the standby CP is being reset. This message is typically generated by a CP that is in the process of becoming the active CP. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

Recommended action

No action is required.

Severity

INFO

PLAT-1002

Message

```
<timestamp>, [PLAT-1002], <sequence-number>,CRITICAL,
<system-name>, CP <Identifies which CP (0 or 1) is
generating the message>: <Error message> CP Fence <CP
Fence register. Contents (2 bytes) are platform-specific>
<CP Error register. Contents are platform-specific> CP
Error <CP Error register. Contents are
platform-specific>.
```

Probable cause

Indicates that the CP cannot access the I2C subsystem either due to an error condtion or being fenced/isolated from the I2C bus.

Recommended action

Reboot the CP if it does not reboot itself. Reseat the CP if rebooting does not solve the problem. If the problem still persists, replace the CP.

Severity

CRITICAL

PLAT-1003

Message

```
<timestamp>, [PLAT-1003], <sequence-number>, FFDC,
CRITICAL, <system-name>, <Info message> Slot <Blade Slot
number> C/BE: <Captured Command/Byte-Enables data> ADBUS:
<Captured AD bus data> misc_intr <Bridge reset
interrupts>.
```

Probable Cause

Indicates a PCI bus hang was detected.

Recommended Action

Try reseating the FRU. If the message persists, the FRU must be replaced.

Severity

CRITICAL

63

PMGR System Messages

This chapter contains information on the following LOG messages:

- PMGR-1001 590
- PMGR-1002 590
- PMGR-1003 590
- PMGR-1004 590
- PMGR-1005 591
- PMGR-1006 591
- PMGR-1007 591
- PMGR-1008 592
- PMGR-1009 592
- PMGR-1010 592

PMGR-1001

Message `<timestamp>, [PMGR-1001], <sequence-number>,, INFO, <system-name>, Switch <FID> was successfully created.`

Probable Cause Indicates the switch with the specified *FID* was successfully created.

Recommended Action No action is required.

Severity INFO

PMGR-1002

Message `<timestamp>, [PMGR-1002], <sequence-number>,, WARNING, <system-name>, Switch <FID> failed to create. Error message: <Error Message>.`

Probable Cause Indicates the switch with the specified *FID* was not created.

Recommended Action No action is required.

Severity WARNING

PMGR-1003

Message `<timestamp>, [PMGR-1003], <sequence-number>,, INFO, <system-name>, Switch <FID> was successfully deleted.`

Probable Cause Indicates the switch with the specified *FID* was successfully deleted.

Recommended Action No action is required.

Severity INFO

PMGR-1004

Message `<timestamp>, [PMGR-1004], <sequence-number>,, WARNING, <system-name>, Switch <FID> failed to delete. Error message: <Error Message>.`

Probable Cause Indicates the switch with the specified *FID* was not deleted.

Recommended Action No action is required.

Severity WARNING

PMGR-1005

Message

```
<timestamp>, [PMGR-1005], <sequence-number>,, INFO,
<system-name>, Ports <Ports> on slot <Slot> to switch
<FID> were moved successfully.
```

Probable Cause Indicates the successful attempt to move the ports to the specified switch.

Recommended Action No action is required.

Severity INFO

PMGR-1006

Message

```
<timestamp>, [PMGR-1006], <sequence-number>,, WARNING,
<system-name>, Moving Ports <Ports> on slot <Slot> to
switch <FID> failed.  Error message: <Error Message>.
```

Probable Cause Indicates the unsuccessful attempt to move the ports to the specified switch.

Recommended Action No action is required.

Severity WARNING

PMGR-1007

Message

```
<timestamp>, [PMGR-1007], <sequence-number>,, INFO,
<system-name>, Switch <FID> was successfully changed to
switch <New FID>.
```

Probable Cause Indicates the successful change of the switch FID.

Recommended Action No action is required.

Severity INFO

PMGR-1008

Message

```
<timestamp>, [PMGR-1008], <sequence-number>,, WARNING,
<system-name>, Switch <FID> failed to change to switch
<New FID>.  Error message: <Error Message>.
```

Probable Cause Indicates the failed attempt to change the switch FID.

Recommended Action No action is required.

Severity WARNING

PMGR-1009

Message

```
<timestamp>, [PMGR-1009], <sequence-number>,, INFO,
<system-name>, The base switch was successfully changed
to switch <FID>.
```

Probable Cause Indicates the successful change of the base switch.

Recommended Action No action is required.

Severity INFO

PMGR-1010

Message

```
<timestamp>, [PMGR-1010], <sequence-number>,, WARNING,
<system-name>, The base switch failed to change to switch
<FID>.  Error message: <Error Message>.
```

Probable Cause Indicates the failed attempt to change the base switch.

Recommended Action No action is required.

Severity WARNING

64

PORT System Messages

This chapter contains information on the following PORT messages:

- PORT-1003 596
- PORT-1004 596
- PORT-1005 597

PORT-1003

Message

```
<timestamp>, [PORT-1003], <sequence-number>,, WARNING,
<system-name>, Port <port number> Faulted because of many
Link Failures
```

Probable cause

Indicates that the specified port is now disabled because the link on this port had multiple failures that exceed an internally set threshold on the port. This problem is typically related to hardware.

Recommended action

Check and replace (if necessary) the hardware attached to both ends of the specified *port number*, including:

- The media (SFPs)
- The cable (fiber optic or copper ISL)
- The attached devices

When finished checking the hardware, perform **portEnable** to reenable the port.

Severity

WARNING

PORT-1004

Message

```
<timestamp>, [PORT-1004], <sequence-number>,, INFO,
<system-name>, Port <port number> could not be enabled
because it is disabled due to long distance.
```

Probable cause

Indicates that the specified port could not be enabled because other ports in the same port group have used up the buffers available for this port group. This happens when other ports were configured to be long distance.

Recommended action

To enable this port, reconfigure the other E_Ports so they are not long distance or change the other E_Ports so they are not E_Ports. This will free some buffers and allow this port to be enabled.

Severity

INFO

PORT-1005

Message

```
<timestamp>, [PORT-1005], <sequence-number>,, WARNING,
<system-name>, Slot <slot number> port <port on slot>
does not support configured L_port. Issue portCfgLport to
clear configuration.
```

Probable cause

Indicates that the specified port is configured to be an L_Port, but that port does not support L_Port. If an L_Port is connected, then the port will be disabled. If an E_Port or F_Port is connected then the port will not come up since it's configured to be an L_Port.

Recommended action

Invoke the **portCfgLport** to clear the L_Port configuration.

Severity

WARNING

65

PS System Messages

This chapter contains information on the following PS messages:

- PS-1000 600
- PS-1001 600
- PS-1002 600
- PS-1003 601
- PS-1004 601
- PS-1005 601
- PS-1006 602

PS-1000

Message

```
<timestamp>, [PS-1000], <sequence-number>, FFDC,
CRITICAL, <system-name>, Failed to initialize Advanced
Performance Monitoring.
```

Probable cause Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor has failed to initialize.

Recommended action The CP should reboot (or fail over) automatically. If it does not, reboot or power cycle the switch to reinitiate the firmware.

Severity CRITICAL

PS-1001

Message

```
<timestamp>, [PS-1001], <sequence-number>,, INFO,
<system-name>, Advanced Performance Monitoring
configuration updated due to change in PID format
```

Probable cause Indicates that the PID format was changed.

Recommended action No action is required. Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information about the PID format.

Severity INFO

PS-1002

Message

```
<timestamp>, [PS-1002], <sequence-number>,, INFO,
<system-name>, Failed to initialize the tracing system
for Advanced Performance Monitoring.
```

Probable cause Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor tracing system has failed to initialize.

Recommended action Tracing will not be available for Advanced Performance Monitoring, but other functions should function normally. To retry activating tracing, reboot (or fail over) the CP.

Severity INFO

PS-1003

Message

```
<timestamp>, [PS-1003], <sequence-number>,, WARNING,
<system-name>, Failed to set end-to-end monitoring mask
on ISL ports.
```

Probable cause

Indicates that the restoring configuration has attempted to set the end-to-end monitoring mask on at least one ISL port.

Recommended action

No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

Severity

WARNING

PS-1004

Message

```
<timestamp>, [PS-1004], <sequence-number>,, WARNING,
<system-name>, Failed to add end-to-end monitors on port
<port> which is an ISL port.
```

Probable cause

Indicates that the restoring configuration has attempted to add end-to-end monitors on at least one ISL port.

Recommended action

No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

Severity

WARNING

PS-1005

Message

```
<timestamp>, [PS-1005], <sequence-number>,, WARNING,
<system-name>, ISL monitor on port <port> stopped
counting because no hardware resources are available
```

Probable cause

Indicates that ISL and end-to-end monitors have used up all hardware resources.

Recommended action

To resume counting, delete some end-to-end monitors sharing the same hardware resource pool.

Severity

WARNING

PS-1006

Message

```
<timestamp>, [PS-1006], <sequence-number>,, WARNING,
<system-name>, Failed to add fabricmode toptalker
monitors on domain=<domain id>, because end-to-end
monitors are configured on this switch.
```

Probable Cause Indicates that end-to-end monitors are configured on the switch.

Recommended Action Delete end-to-end monitors on that switch and re-install fabricmode TopTalker monitor. End-to-end monitors and fabricmode toptalker monitors are mutually exclusive.

Severity WARNING

66

PSWP System Messages

This chapter contains information on the following PSWP messages:

- PSWP-1001 604
- PSWP-1002 604
- PSWP-1003 604

PSWP-1001

Message `<timestamp>, [PSWP-1001], <sequence-number>,, INFO, <system-name>, Areas for port <wwn name corresponding to source port> and port <wwn name corresponding to destination port> are swapped. New area for port <wwn name corresponding to source port> is <wwn name corresponding to destination port> and port <new area corresponding to source wwn> is <new area corresponding to destination wwn>.`

Probable cause Indicates that the **portSwap** command has been issued.

Recommended action No action is required.

Severity INFO

PSWP-1002

Message `<timestamp>, [PSWP-1002], <sequence-number>,, INFO, <system-name>, Port Swap feature enabled.`

Probable cause Indicates that the **portSwap** feature has been enabled in the switch.

Recommended action No action is required.

Severity INFO

PSWP-1003

Message `<timestamp>, [PSWP-1003], <sequence-number>,, INFO, <system-name>, Port Swap feature disabled.`

Probable cause Indicates that the **portSwap** feature has been disabled in the switch.

Recommended action No action is required.

Severity INFO

67

RAS System Messages

This chapter contains information on the following RAS messages:

- RAS-1001 606
- RAS-1002 606
- RAS-1004 606
- RAS-1004 606
- RAS-1005 607
- RAS-1006 607
- RAS-2001 607
- RAS-2002 608
- RAS-2003 608
- RAS-3001 608
- RAS-3002 609
- RAS-3003 609
- RAS-3004 609

RAS-1001

Message

```
<timestamp>, [RAS-1001], <sequence-number>,, INFO,
<system-name>, First failure data capture (FFDC) event
occurred.
```

Probable cause Indicates that a failure happened and the failure data was captured.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

RAS-1002

Message

```
<timestamp>, [RAS-1002], <sequence-number>,, WARNING,
<system-name>, First failure data capture (FFDC) maximum
storage size (<log size limit> MB) was reached.
```

Probable cause Indicates that the maximum storage size for FFDC data capture is reached.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

RAS-1004

Message

```
<timestamp>, [RAS-1004], <sequence-number>, FFDC,
WARNING, <system-name>, Software 'verify' error detected.
```

Probable cause Indicates an internal software error.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

RAS-1005

Message

```
<timestamp>, [RAS-1005], <sequence-number>, FFDC,
WARNING, <system-name>, Software 'assert' error detected.
```

Probable cause

Indicates a internal software error.

Recommended action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

RAS-1006

Message

```
<timestamp>, [RAS-1006], <sequence-number>,, INFO,
<system-name>, Support data file (<Uploaded file name>)
automatically transferred to remote address ' <Remote
target designated by user> '.
```

Probable Cause

Indicates that the support data file is transferred from the switch automatically.

Recommended Action

No action is required.

Severity

INFO

RAS-2001

Message

```
<timestamp>, [RAS-2001], <sequence-number>,, INFO,
<system-name>, Audit message log is enabled.
```

Probable Cause

A user has enabled the audit message log.

Recommended Action

No action is required.

Severity

INFO

RAS-2002

Message `<timestamp>, [RAS-2002], <sequence-number>,, INFO, <system-name>, Audit message log is disabled.`

Probable Cause A user has disabled the audit message log.

Recommended Action No action is required.

Severity INFO

RAS-2003

Message `<timestamp>, [RAS-2003], <sequence-number>,, INFO, <system-name>, Audit message class configuration has been changed to <New audit class configuration>.`

Probable Cause A user has changed the configured classes of the audit feature.

Recommended Action No action is required.

Severity INFO

RAS-3001

Message `<timestamp>, [RAS-3001], <sequence-number>,, INFO, <system-name>, USB storage device plug-in detected.`

Probable Cause Indicates that the USB storage device plug-in is being detected.

Recommended Action No action is required.

Severity INFO

RAS-3002

Message `<timestamp>, [RAS-3002], <sequence-number>,, INFO, <system-name>, USB storage device enabled.`

Probable Cause Indicates that the USB storage device is enabled.

Recommended Action No action is required.

Severity INFO

RAS-3003

Message `<timestamp>, [RAS-3003], <sequence-number>,, WARNING, <system-name>, USB storage device was unplugged before it was disabled.`

Probable Cause Indicates that the USB storage device was unplugged before it was disabled.

Recommended Action No action is required.

Severity WARNING

RAS-3004

Message `<timestamp>, [RAS-3004], <sequence-number>,, INFO, <system-name>, USB storage device disabled.`

Probable Cause Indicates that the USB storage device is disabled.

Recommended Action No action is required.

Severity INFO

68

RCS System Messages

This chapter contains information on the following RCS messages:

- RCS-1001 612
- RCS-1002 612
- RCS-1003 612
- RCS-1004 613
- RCS-1005 613
- RCS-1006 614
- RCS-1007 614
- RCS-1008 615

RCS-1001

Message

```
<timestamp>, [RCS-1001], <sequence-number>,, INFO,
<system-name>, RCS has been disabled. Some switches in
the fabric do not support this feature.
```

Probable cause

Indicates that the RCS feature has been disabled on the local switch because not all switches in the fabric support RCS or the switch is in nonnative mode.

Recommended action

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

Run the **firmwareDownload** command to update the firmware for any switches that do not support RCS.

Severity

INFO

RCS-1002

Message

```
<timestamp>, [RCS-1002], <sequence-number>,, INFO,
<system-name>, RCS has been enabled.
```

Probable cause

Indicates that the RCS feature has been enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

Recommended action

No action is required.

Severity

INFO

RCS-1003

Message

```
<timestamp>, [RCS-1003], <sequence-number>,, ERROR,
<system-name>, Failed to allocate memory: (<function
name>)
```

Probable cause

Indicates that the specified RCS function failed to allocate memory.

Recommended action

This message is usually transitory. Wait a few minutes and retry the command.

Check memory usage on the switch using the **memShow** command.

Reboot or power cycle the switch.

Severity ERROR

RCS-1004

Message

```
<timestamp>, [RCS-1004], <sequence-number>,, ERROR,
<system-name>, Application(<application name>) not
registered.(<error string>)
```

Probable cause Indicates that a specified application did not register with RCS.

Recommended action Run the **haShow** command to view the HA state.

Run the **haDisable** and the **haEnable** commands.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and greater, v4.1 and greater.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

Severity ERROR

RCS-1005

Message

```
<timestamp>, [RCS-1005], <sequence-number>,, INFO,
<system-name>, Phase <RCS phase>, <Application Name>
Application returned <Reject reason>, 0x<Reject code>.
```

Probable cause Indicates that a receiving switch is rejecting an RCS phase.

Recommended action If the reject is in ACA phase, wait several minutes and then retry the operation from the sender switch.

If the reject is in the SFC phase, check if the application license exists for the local domain and if the application data is compatible.

Severity INFO

RCS-1006

Message

```
<timestamp>, [RCS-1006], <sequence-number>,, INFO,
<system-name>, State <RCS phase>, Application
<Application Name> AD<Administrative Domain>, RCS CM.
Domain <Domain ID that sent the reject> returned
0x<Reject code>.
```

Probable cause

Indicates that a remote domain rejected an RCS phase initiated by an application on the local switch.

If the reject phase is ACA, the remote domain might be busy and could not process the new request.

If the reject phase is SFC, the data sent by the application might not be compatible or the domain does not have the license to support that application.

Recommended action

If the reject is in ACA phase, wait several minutes and then retry the operation.

If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

Severity

INFO

RCS-1007

Message

```
<timestamp>, [RCS-1007], <sequence-number>,, ERROR,
<system-name>, Zone DB size and propogation overhead
exceeds domain <domain number>'s maximum supported Zone
DB size <max zone db size>. Retry after reducing the Zone
DB size.
```

Probable cause

Indicates that a domain cannot handle the zone database being committed.

Recommended action

Reduce the zone database size.

Severity

ERROR

RCS-1008

Message `<timestamp>, [RCS-1008], <sequence-number>,, ERROR, <system-name>, Domain <domain number> Lowest Max Zone DB size`

Probable cause Indicates that the specified domain has the lowest maximum Zone database size.

Recommended action Reduce the zone database size.

Severity ERROR

69

RKD System Messages

This chapter contains information on the following RKD messages:

- RKD-1001 618
- RKD-1002 618
- RKD-1003 618

RKD-1001

Message

```
<timestamp>, [RKD-1001], <sequence-number>,, INFO,
<system-name>, <Re-key type (First time
encryption/Rekey/Write Metadata)> operation <Re-key
action (started/completed/cancelled)>.\nTarget: <Target
physial WWN>, Initiator: <Initiator physical WWN>, LUN
ID: <LUN ID>.\n SessionId:<Session ID>/<Session MN>
```

Probable Cause Indicates that a First time encryption/re-key/Write Metadata was started/completed/cancelled.

Recommended Action No action is required.

Severity INFO

RKD-1002

Message

```
<timestamp>, [RKD-1002], <sequence-number>,, ERROR,
<system-name>, Could not start <Re-key type (First time
encryption/Rekey/Write Metadata)> operation.\n<I/T/L
String>.\n No response from cluster member WWN: <EE WWN>
Slot: <EE Slot Number>.
```

Probable Cause Indicates that a First time encryption/re-key/Write Metadata was not started.

Recommended Action Correct the Cluster Ethernet link error and retry.

Severity ERROR

RKD-1003

Message

```
<timestamp>, [RKD-1003], <sequence-number>,, CRITICAL,
<system-name>, <Re-key type (First time
encryption/Rekey/Write Metadata)> encountered a FATAL
SCSI error and will be suspended.\n<I/T/L
String>.\nCommand: <Read/Write>\nLBA: <LBA>\nNum Blocks:
<Num of Blocks>\nError: <Error String>\nSK/ASC: <SCSI
Sense Key>/<SCSI ASC>.
```

Probable Cause Indicates that a First time encryption/re-key/Write Metadata encountered a fatal SCSI error and was suspended.

Recommended Action Correct the error and resume.

Severity CRITICAL

70

RPCD System Messages

This chapter contains information on the following RPCD messages:

- RPCD-1001 622
- RPCD-1002 622
- RPCD-1003 622
- RPCD-1004 623
- RPCD-1005 623
- RPCD-1006 623
- RPCD-1007 624

RPCD-1001

Message `<timestamp>, [RPCD-1001], <sequence-number>,, WARNING, <system-name>, Authentication Error: client \"<IP address>\" has bad credentials: <bad user name and password pair>`

Probable cause Indicates that an authentication error was reported. The specified *client IP address* has faulty credentials.

Recommended action Enter the correct user name and password from the Fabric Access API host.

Severity WARNING

RPCD-1002

Message `<timestamp>, [RPCD-1002], <sequence-number>,, WARNING, <system-name>, Missing certificate file. Secure RPCd is disabled.`

Probable cause Indicates that an SSL certificate is missing.

Recommended action To enable RPCD in Secure mode, install a valid SSL certificate on the switch.

Severity WARNING

RPCD-1003

Message `<timestamp>, [RPCD-1003], <sequence-number>,, WARNING, <system-name>, Permission denied accessing certificate file. Secure RPCd is disabled.`

Probable cause Indicates that the SSL certificate file configured on the switch could not be accessed because root did not have read-level access.

Recommended action Change the file system access level for the certificate file to have root read-level access.

Severity WARNING

RPCD-1004

Message

```
<timestamp>, [RPCD-1004], <sequence-number>,, WARNING,
<system-name>, Invalid certificate file. Secure RPCd is
disabled.
```

Probable cause

Indicates that the SSL certificate file has been corrupted.

Recommended action

To enable RPCD in Secure mode, install a valid SSL certificate the switch.

Severity

WARNING

RPCD-1005

Message

```
<timestamp>, [RPCD-1005], <sequence-number>,, WARNING,
<system-name>, Missing private key file. Secure RPCd is
disabled.
```

Probable cause

Indicates that the private key file is missing.

Recommended action

Run the **pkiCreate** command to install a valid private key file.

Severity

WARNING

RPCD-1006

Message

```
<timestamp>, [RPCD-1006], <sequence-number>,, WARNING,
<system-name>, Permission denied accessing private key
file. Secure RPCd is disabled.
```

Probable cause

Indicates that the private key file configured on the switch could not be accessed because root did not have read-level access.

Recommended action

Change the file system access level for the private key file and make sure that root has read-level access.

Severity

WARNING

RPCD-1007

Message

```
<timestamp>, [RPCD-1007], <sequence-number>,, WARNING,
<system-name>, Invalid private file. Secure RPCd is
disabled.
```

Probable cause

Indicates that the private key file has been corrupted.

Recommended action

Run the **pkiCreate** command to install a valid private key file.

Severity

WARNING

71

RTWR System Messages

This chapter contains information on the following RTWR messages:

- RTWR-1001 626
- RTWR-1002 626
- RTWR-1003 627

RTWR-1001

Message

```
<timestamp>, [RTWR-1001], <sequence-number>,, ERROR,
<system-name>, RTWR <routine: error message> 0x<detail
1>, 0x<detail 2>, 0x<detail 3>, 0x<detail 4>, 0x<detail
5>
```

Probable cause

Indicates that an error occurred in the RTWR. The message provides the name of the routine having the error, and more specific error information. The values in details 1 through 5 might provide more information.

Recommended action

No action is required.

Severity

ERROR

RTWR-1002

Message

```
<timestamp>, [RTWR-1002], <sequence-number>,, WARNING,
<system-name>, RTWR <error message> 0x<detail1>,
0x<detail2>, 0x<detail3>, 0x<detail4>, 0x<detail5>
```

Probable cause

Indicates that the RTWR has exhausted the maximum number of retries sending data to the specified domain. Possible detail values include:

- RTWRTransmit: Max retries exhausted
- detail1: Port
- detail2: Domain
- detail3: Retry Count
- detail4: Status
- detail5: Process ID

Recommended action

Run the **fabricShow** command to see if the specified domain ID is online.

Enable the switch with the specified domain ID.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

RTWR-1003

Message

```
<timestamp>, [RTWR-1003], <sequence-number>,, INFO,
<system-name>, <module name>: RTWR retry <number of times
retried> to domain <domain ID>, iu_data <first word of
iu_data>
```

Probable cause Indicates how many times RTWR failed to get a response and retried.

Recommended action Run the **dom** command to verify that the specified domain ID is reachable.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

72 SAS System Messages

This chapter contains information on the following SAS message:

- SAS-1001 630

SAS-1001

Message

```
<timestamp>, [SAS-1001], <sequence-number>,, ERROR,
<system-name>, string description of command which
failed> of GE <GE port number which failed> failed.
Please retry the command. Data inst=<chip instance>
st=<chip init state> rsn=<failure reason> fn=<message
function> oid=<chip OID>.
```

Probable cause

The hardware is not responding to the command request; possibly because it is busy.

Recommended action

Retry the command.

Severity

ERROR

73

SCN System Messages

This chapter contains information on the following SCN message:

- SCN-1001 632

SCN-1001

Message

```
<timestamp>, [SCN-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, SCN queue overflow for process
<daemon name>
```

Probable cause

Indicates that an attempt to write a state change notification (SCN) message to a specific queue has failed because the SCN queue for the specified *daemon name* is full. This might be caused by the daemon hanging or if the system is busy.

The valid values for *daemon name* can be:

- fabricd
- asd
- evmd
- fcpd
- webd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

Recommended action

If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

74

SEC System Messages

This chapter contains information on the following SEC messages:

- SEC-1001 638
- SEC-1002 638
- SEC-1003 639
- SEC-1005 639
- SEC-1006 640
- SEC-1007 640
- SEC-1008 641
- SEC-1009 641
- SEC-1016 641
- SEC-1022 642
- SEC-1024 642
- SEC-1025 642
- SEC-1026 643
- SEC-1028 643
- SEC-1029 644
- SEC-1030 644
- SEC-1031 645
- SEC-1032 645
- SEC-1033 645
- SEC-1034 646
- SEC-1035 646
- SEC-1036 646
- SEC-1037 647
- SEC-1038 647
- SEC-1040 647
- SEC-1041 648
- SEC-1042 648

- SEC-1043 648
- SEC-1044 649
- SEC-1045 649
- SEC-1046 650
- SEC-1049 650
- SEC-1050 650
- SEC-1051 651
- SEC-1052 651
- SEC-1053 652
- SEC-1054 652
- SEC-1055 653
- SEC-1056 653
- SEC-1057 653
- SEC-1059 654
- SEC-1062 654
- SEC-1063 655
- SEC-1064 655
- SEC-1065 655
- SEC-1069 656
- SEC-1071 656
- SEC-1072 656
- SEC-1073 657
- SEC-1074 657
- SEC-1075 657
- SEC-1076 658
- SEC-1077 658
- SEC-1078 658
- SEC-1079 659
- SEC-1080 659
- SEC-1081 660
- SEC-1082 660
- SEC-1083 660
- SEC-1084 661
- SEC-1085 661
- SEC-1086 661
- SEC-1087 662
- SEC-1088 662
- SEC-1089 662
- SEC-1090 663
- SEC-1091 663
- SEC-1092 663
- SEC-1093 664
- SEC-1094 664

- SEC-1095 665
- SEC-1096 665
- SEC-1097 665
- SEC-1098 666
- SEC-1099 666
- SEC-1100 666
- SEC-1101 667
- SEC-1102 667
- SEC-1104 668
- SEC-1105 668
- SEC-1106 668
- SEC-1107 669
- SEC-1108 669
- SEC-1110 670
- SEC-1111 670
- SEC-1112 670
- SEC-1113 671
- SEC-1114 671
- SEC-1115 671
- SEC-1116 672
- SEC-1117 672
- SEC-1118 672
- SEC-1119 673
- SEC-1121 673
- SEC-1122 673
- SEC-1123 674
- SEC-1124 674
- SEC-1126 674
- SEC-1130 675
- SEC-1135 675
- SEC-1136 675
- SEC-1137 676
- SEC-1138 677
- SEC-1139 677
- SEC-1142 677
- SEC-1145 678
- SEC-1146 678
- SEC-1153 679
- SEC-1154 679
- SEC-1155 679
- SEC-1156 680
- SEC-1157 680
- SEC-1158 681

- SEC-1159 681
- SEC-1160 681
- SEC-1163 682
- SEC-1164 682
- SEC-1165 682
- SEC-1166 683
- SEC-1167 683
- SEC-1168 683
- SEC-1170 684
- SEC-1171 684
- SEC-1172 685
- SEC-1173 685
- SEC-1174 685
- SEC-1175 686
- SEC-1176 686
- SEC-1180 686
- SEC-1181 687
- SEC-1182 687
- SEC-1183 687
- SEC-1184 688
- SEC-1185 688
- SEC-1186 688
- SEC-1187 689
- SEC-1188 689
- SEC-1189 690
- SEC-1190 690
- SEC-1191 691
- SEC-1192 691
- SEC-1193 692
- SEC-1194 692
- SEC-1195 692
- SEC-1196 693
- SEC-1197 693
- SEC-1198 694
- SEC-1199 694
- SEC-1200 695
- SEC-1201 695
- SEC-1202 696
- SEC-1203 696
- SEC-1250 696
- SEC-1251 697
- SEC-1253 697
- SEC-1300 698

- SEC-1301 698
- SEC-1302 698
- SEC-1303 699
- SEC-1304 699
- SEC-1305 699
- SEC-1306 700
- SEC-1307 700
- SEC-1308 701
- SEC-1309 701
- SEC-1310 701
- SEC-1311 702
- SEC-1312 702
- SEC-1313 702
- SEC-1314 703
- SEC-1315 703
- SEC-1316 704
- SEC-1317 704
- SEC-1318 704
- SEC-1319 705
- SEC-1320 705
- SEC-1321 705
- SEC-1322 706
- SEC-1323 706
- SEC-1324 706
- SEC-1325 707
- SEC-1326 707
- SEC-1327 708
- SEC-1328 708
- SEC-1329 708
- SEC-1330 709
- SEC-1331 709
- SEC-1332 710
- SEC-1333 710
- SEC-3035 710
- SEC-3036 711
- SEC-3037 711
- SEC-3038 711
- SEC-3039 712
- SEC-3050 712
- SEC-3051 712

SEC-1001

Message

```
<timestamp>, [SEC-1001], <sequence-number>,, ERROR,
<system-name>, RCS process fails: <reason code>
```

Probable cause

Indicates that the reliable commit service (RCS) process fails to complete. RCS is a mechanism for transferring data from one switch to other switches within the fabric. RCS ensures that either all or none of the switches commit to the database. RCS can fail if one switch in the fabric is busy or in an error state that prevents it from accepting the database.

Recommended action

RCS process is evoked when the security database is modified by a security command (for example, **secPolicySave**, **secPolicyActivate**, or **secVersionReset**). If the switch is busy, the command might fail the first time. Retry the command.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, RCS is automatically enabled.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

SEC-1002

Message

```
<timestamp>, [SEC-1002], <sequence-number>,, ERROR,
<system-name>, Security data fails: <Reason Text>.
```

Probable cause

Indicates that the receiving switch fails to validate the security database sent from the primary fabric configurations server (FCS) switch. This might be caused by several factors: the data package may be corrupted, the time stamp on the package may be out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure may result from an internal error, such as losing the primary public key or an invalid database.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in *Ready* state. If a switch is in

the error state, the database might not be correctly updated for that switch. The error might also be a result of an internal corruption or a hacker attack to the secure fabric. If you have reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

Severity ERROR

SEC-1003

Message

```
<timestamp>, [SEC-1003], <sequence-number>,, WARNING,
<system-name>, Fail to download security data to domain
<Domain number> after <Number of retires> retries
```

Probable cause Indicates that the specified domain failed to download security data after the specified number of attempts, and that the failed switch encountered an error accepting the database download. The primary switch will segment the failed switch after 30 tries.

Recommended action Reset the version stamp on the switch to 0 using the **secVersionReset** command and then rejoin the switch to the fabric.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

SEC-1005

Message

```
<timestamp>, [SEC-1005], <sequence-number>,, INFO,
<system-name>, Primary FCS receives data request from
domain <Domain number>
```

Probable cause Indicates that the primary fabric configurations server (FCS) received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resync with the rest of the switches in the fabric.

Recommended action Use the **secFabricShow** command to check whether any of the switches in the fabric encountered an error. If one or more switches is not in *Ready* state, and you have reason to believe that the error is the

result of a possible security breach, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1006

Message

```
<timestamp>, [SEC-1006], <sequence-number>,, WARNING,
<system-name>, Security statistics error: Failed to reset
due to invalid <data>.
```

Probable cause Indicates that invalid data has been received for any statistic-related command for security (**secStatsShow** or **secStatsReset**). The counter is updated automatically when a security violation occurs. This message might also occur if the updating counter fails.

Recommended action If the message is the result of a user command, retry the statistic command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

SEC-1007

Message

```
<timestamp>, [SEC-1007], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address of the violating host> tries to
establish API connection.
```

Probable cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended action Check for unauthorized access to the switch through the API connection.

Severity INFO

SEC-1008

Message

```
<timestamp>, [SEC-1008], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address of the violating host> tries to
establish HTTP connection.
```

Probable cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended action Check for unauthorized access to the switch through the HTTP connection.

Severity INFO

SEC-1009

Message

```
<timestamp>, [SEC-1009], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address of the violating host> tries to
establish TELNET connection.
```

Probable cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended action Check for unauthorized access to the switch through the telnet connection.

Severity INFO

SEC-1016

Message

```
<timestamp>, [SEC-1016], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address of the violating host> tries to
establish SSH connection.
```

Probable cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended action Check for unauthorized access to the switch through the SSH connection.

Severity INFO

SEC-1022

Message `<timestamp>, [SEC-1022], <sequence-number>,, WARNING, <system-name>, Failed to <operation> PKI objects.`

Probable cause Indicates that the fabric failed to generate or validate either the public or private key pair or the certificate signing request (CSR).

Recommended action Run the **pkiShow** command and verify that all public key infrastructure (PKI) objects exist on the switch. If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

Severity WARNING

SEC-1024

Message `<timestamp>, [SEC-1024], <sequence-number>,, INFO, <system-name>, The <DB name> security database is too large to fit in flash.`

Probable cause Indicates that the size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

Recommended action Reduce the size of the security database by reducing the number of entries within each policy.

Severity INFO

SEC-1025

Message `<timestamp>, [SEC-1025], <sequence-number>,, ERROR, <system-name>, Invalid IP address (<IP address>) detected.`

Probable cause Indicates that a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configurations server (FCS) distributes the security database to the

other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1026

Message

```
<timestamp>, [SEC-1026], <sequence-number>,, ERROR,
<system-name>, Invalid format or character in switch
member <switch member ID>.
```

Probable cause Indicates that a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configurations server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1028

Message

```
<timestamp>, [SEC-1028], <sequence-number>,, ERROR,
<system-name>, No name is specified.
```

Probable cause Indicates that a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configurations server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is

in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1029

Message

```
<timestamp>, [SEC-1029], <sequence-number>,, ERROR,
<system-name>, Invalid character in <policy name>.
```

Probable cause Indicates that a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configurations server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1030

Message

```
<timestamp>, [SEC-1030], <sequence-number>, ERROR,
<system-name>, The length of the name invalid.
```

Probable cause Indicates that a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configurations server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1031

Message

```
<timestamp>, [SEC-1031], <sequence-number>,, WARNING,
<system-name>, Current security policy DB cannot be
supported by standby. CPs will go out of sync.
```

Probable cause

Indicates that the security database size is not supported by the standby control processor (CP).

Recommended action

Reduce the security policy size by deleting entries within a policy or by deleting some policies.

Severity

WARNING

SEC-1032

Message

```
<timestamp>, [SEC-1032], <sequence-number>,, ERROR,
<system-name>, Empty FCS list is not allowed.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1033

Message

```
<timestamp>, [SEC-1033], <sequence-number>,, ERROR,
<system-name>, Invalid character used in member parameter
to add switch to SCC policy; command terminated.
```

Probable cause

Indicates that a member parameter in the **secPolicyAdd** command is invalid (e. g., it may include an invalid character, such as an asterisk). A valid switch identifier (a WWN, a domain ID, or a switch name) must be provided as a member parameter in the **secPolicyAdd**

command. Only the **secPolicyCreate** command supports use of the asterisk for adding switches to policies.

Recommended action Run the **secPolicyAdd** command using a valid switch identifier (WWN, domain ID, or switch name) to add specific switches to the switch connection control (SCC) policy.

Severity ERROR

SEC-1034

Message

```
<timestamp>, [SEC-1034], <sequence-number>,, ERROR,
<system-name>, Invalid member <policy member>.
```

Probable cause Indicates that the input list has an invalid member.

Recommended action Verify the member names, and input the correct information.

Severity ERROR

SEC-1035

Message

```
<timestamp>, [SEC-1035], <sequence-number>,, ERROR,
<system-name>, Invalid device WWN <device WWN>.
```

Probable cause Indicates that the specified world-wide name (WWN) is invalid.

Recommended action Enter the correct WWN value.

Severity ERROR

SEC-1036

Message

```
<timestamp>, [SEC-1036], <sequence-number>,, ERROR,
<system-name>, Device name <device name> is invalid due
to a missing colon.
```

Probable cause Indicates that one or more device names mentioned in the **securePolicyCreate** or **securePolicyAdd** command does not having the colon character as required.

Recommended action Run the **secPolicyCreate** or **secPolicyAdd** command with a properly formatted device name parameter.

Severity ERROR

SEC-1037

Message `<timestamp>, [SEC-1037], <sequence-number>,, ERROR, <system-name>, Invalid WWN format <invalid WWN>.`

Probable cause Indicates that the world-wide name (WWN) entered in the policy member list had an invalid format.

Recommended action Run the command again using the standard WWN format, 16 hexadecimal digits grouped as eight colon separated pairs. For example: 50:06:04:81:D6:F3:45:42.

Severity ERROR

SEC-1038

Message `<timestamp>, [SEC-1038], <sequence-number>,, ERROR, <system-name>, Invalid domain <domain ID>.`

Probable cause Indicates that an invalid domain ID was entered.

Recommended action Verify that the domain ID is correct, if not, then re-run the command using the correct domain ID.

Severity ERROR

SEC-1040

Message `<timestamp>, [SEC-1040], <sequence-number>,, ERROR, <system-name>, Invalid portlist (<port list>). Cannot combine * with port member in the same portlist.`

Probable cause Indicates that the port list contains the wildcard asterisk (*) character. You cannot use the asterisk in a port list.

Recommended action Enter the port list values without any wildcards.

Severity ERROR

SEC-1041

Message `<timestamp>, [SEC-1041], <sequence-number>,, ERROR, <system-name>, Invalid port member <port member> in portlist (<port list>). <Reason>.`

Probable cause Indicates that the port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

Recommended action Use valid syntax when entering port members.

Severity ERROR

SEC-1042

Message `<timestamp>, [SEC-1042], <sequence-number>,, ERROR, <system-name>, Invalid index/area member <port member> in portlist (<Port list>). Out of range (<Minimum value> - <Maximum value>).`

Probable cause Indicates that the specified index or area member is not within the minimum and maximum range.

Recommended action Use valid syntax when entering index or area numbers.

Severity ERROR

SEC-1043

Message `<timestamp>, [SEC-1043], <sequence-number>,, ERROR, <system-name>, Invalid port range <Minimum> - <Maximum>.`

Probable cause Indicates that the specified port is not within the minimum and maximum range.

Recommended action Use valid syntax when entering port ranges.

Severity ERROR

SEC-1044

Message

```
<timestamp>, [SEC-1044], <sequence-number>,, ERROR,
<system-name>, Duplicate member <member ID> in (<List>).
```

Probable cause Indicates that the specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

Recommended action Do not specify any duplicates.

Severity ERROR

SEC-1045

Message

```
<timestamp>, [SEC-1045], <sequence-number>,, ERROR,
<system-name>, Too many port members.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1046

Message

```
<timestamp>, [SEC-1046], <sequence-number>,, ERROR,
<system-name>, Empty list.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1049

Message

```
<timestamp>, [SEC-1049], <sequence-number>,, ERROR,
<system-name>, Invalid switch name <switch name>.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1050

Message

```
<timestamp>, [SEC-1050], <sequence-number>,, ERROR,
<system-name>, There are more than one switches with the
same name <switch name> in the fabric.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1051

Message

```
<timestamp>, [SEC-1051], <sequence-number>,, ERROR,
<system-name>, Missing brace for port list <port list>.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1052

Message

```
<timestamp>, [SEC-1052], <sequence-number>,, ERROR,
<system-name>, Invalid input.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1053

Message

```
<timestamp>, [SEC-1053], <sequence-number>,, ERROR,
<system-name>, Invalid pFCS list <pFCS list>
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1054

Message

```
<timestamp>, [SEC-1054], <sequence-number>,, ERROR,
<system-name>, Invalid FCS list length <list length>
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1055

Message

```
<timestamp>, [SEC-1055], <sequence-number>,, ERROR,
<system-name>, Invalid FCS list <WWN list>
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1056

Message

```
<timestamp>, [SEC-1056], <sequence-number>,, ERROR,
<system-name>, Invalid position <New position>. Only
<Number of members in FCS list> members in list.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1057

Message

```
<timestamp>, [SEC-1057], <sequence-number>,, ERROR,
<system-name>, No change. Both positions are the same.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1059

Message

```
<timestamp>, [SEC-1059], <sequence-number>,, ERROR,
<system-name>, Fail to <operation, e.g., save, delete,
etc.,> <named item> to flash.
```

Probable cause Indicates that the operation failed when writing to flash.

Recommended action Run the **supportFtp - e** command to FTP files from the switch and remove them from the flash.

Severity ERROR

SEC-1062

Message

```
<timestamp>, [SEC-1062], <sequence-number>,, ERROR,
<system-name>, Invalid number of Domains in Domain List.
```

Probable cause Indicates either that no domains or domains more than the maximum number supported are specified.

Recommended action Enter the correct number of domains.

Severity ERROR

SEC-1063

Message `<timestamp>, [SEC-1063], <sequence-number>,, ERROR, <system-name>, Failed to reset statistics.`

Probable cause Indicates that either the type or domains specified are invalid.

Recommended action Enter valid input.

Severity ERROR

SEC-1064

Message `<timestamp>, [SEC-1064], <sequence-number>,, ERROR, <system-name>, Failed to sign message.`

Probable cause Indicates that the public key infrastructure (PKI) objects on the switch are not in a valid state and the signature operation failed.

Recommended action Run the **pkiShow** command to verify that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

Severity ERROR

SEC-1065

Message `<timestamp>, [SEC-1065], <sequence-number>,, ERROR, <system-name>, Invalid character in list.`

Probable cause Indicates that the input list has an invalid character.

Recommended action Enter valid input.

Severity ERROR

SEC-1069

Message `<timestamp>, [SEC-1069], <sequence-number>,, ERROR, <system-name>, Security Database is corrupted.`

Probable cause Indicates that the security database is corrupted for unknown reasons.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1071

Message `<timestamp>, [SEC-1071], <sequence-number>,, ERROR, <system-name>, No new security policy data to apply.`

Probable cause Indicates that no changes in the defined security policy database need to be activated at this time.

Recommended action Verify that the security event was planned. First change some policy definitions, then run the **secPolicyActivate** command to activate the policies.

Severity ERROR

SEC-1072

Message `<timestamp>, [SEC-1072], <sequence-number>,, ERROR, <system-name>, <Policy type> Policy List is Empty!`

Probable cause Indicates that the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1073

Message

```
<timestamp>, [SEC-1073], <sequence-number>,, ERROR,
<system-name>, No FCS policy in list!
```

Probable cause

Indicates that the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

SEC-1074

Message

```
<timestamp>, [SEC-1074], <sequence-number>,, ERROR,
<system-name>, Cannot execute the command on this switch.
Check the secure mode and FCS status.
```

Probable cause

Indicates that a security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have required fabric configurations server (FCS) privilege.

Recommended action

If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has required privilege, that is, either a backup FCS or primary FCS.

Severity

ERROR

SEC-1075

Message

```
<timestamp>, [SEC-1075], <sequence-number>,, ERROR,
<system-name>, Fail to <operation> new policy set on all
switches.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1076

Message `<timestamp>, [SEC-1076], <sequence-number>,, ERROR, <system-name>, NoNodeWWNZoning option has been changed.`

Probable cause Indicates that the NoNodeWWNZoning option has been changed. If the option is turned on, a zone member can be added using node WWNs, but the member will not be able to communicate with others nodes in the zone.

Recommended action Reenable the current zone configuration for the change to take effect.

Severity ERROR

SEC-1077

Message `<timestamp>, [SEC-1077], <sequence-number>,, ERROR, <system-name>, Failed to activate new policy set on all switches.`

Probable cause Indicates that the policy could not be activated. Possible reasons that the policy could not be activate include not enough memory or a busy switch.

Recommended action Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

Severity ERROR

SEC-1078

Message `<timestamp>, [SEC-1078], <sequence-number>,, ERROR, <system-name>, No new data to abort.`

Probable cause Indicates that there are no new changes in the defined security policy database that can be aborted.

Recommended action Verify that security event was planned. Verify if there were really any changes to the defined policy database that can be aborted.

Severity ERROR

SEC-1079

Message

```
<timestamp>, [SEC-1079], <sequence-number>,, ERROR,
<system-name>, The policy name <policy name> is invalid.
```

Probable cause Indicates that the policy name entered in the **secPolicyCreate | Activate | Add | Delete** command was invalid.

Recommended action Run the command again using a valid policy name.

Severity ERROR

SEC-1080

Message

```
<timestamp>, [SEC-1080], <sequence-number>,, ERROR,
<system-name>, Operation denied. Please, use
secModeEnable command.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1081

Message `<timestamp>, [SEC-1081], <sequence-number>,, ERROR, <system-name>, Entered a name for a DCC policy ID that was not unique.`

Probable cause Indicates that the device connection control (DCC) policy name given in the **secPolicyCreate** command was the same as another DCC policy.

Recommended action Make sure that the DCC policy name has a unique alpha-numeric string, and run the **secPolicyCreate** command again.

Severity ERROR

SEC-1082

Message `<timestamp>, [SEC-1082], <sequence-number>,, ERROR, <system-name>, Failed to create <policy name> policy.`

Probable cause Indicates that the security policy was not created due to faulty input or low resources.

Recommended action Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.

Severity ERROR

SEC-1083

Message `<timestamp>, [SEC-1083], <sequence-number>,, ERROR, <system-name>, Name already exists.`

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is

in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1084

Message

```
<timestamp>, [SEC-1084], <sequence-number>,, ERROR,
<system-name>, Name exists for different type <Policy
name>.
```

Probable cause Indicates that the specified policy already exists.

Recommended action No action is required.

Severity ERROR

SEC-1085

Message

```
<timestamp>, [SEC-1085], <sequence-number>,, ERROR,
<system-name>, Failed to create <policy name>.
```

Probable cause Indicates that the security policy was not created.

Recommended action Check that the current policy configuration is valid. For example, the RSNMP policy cannot exist without the WSNMP policy.

Severity ERROR

SEC-1086

Message

```
<timestamp>, [SEC-1086], <sequence-number>,, ERROR,
<system-name>, The security database is too large to fit
in flash.
```

Probable cause Indicates that the security database has more data than the flash can accommodate.

Recommended action Reduce the number of entries in some policies to decrease the security database size.

Severity ERROR

SEC-1087

Message

```
<timestamp>, [SEC-1087], <sequence-number>,, ERROR,
<system-name>, The security database is larger than the
data distribution limit of fabric <fabric data
distribution limit> bytes.
```

Probable cause Indicates that the security database has more data than can be distributed to some of the switches in the fabric.

Recommended action Reduce the number of entries in the security policies to decrease the security database size.

Severity ERROR

SEC-1088

Message

```
<timestamp>, [SEC-1088], <sequence-number>,, ERROR,
<system-name>, Cannot execute the command. Please try
later.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1089

Message

```
<timestamp>, [SEC-1089], <sequence-number>,, ERROR,
<system-name>, Policy name <policy name> was not found.
```

Probable cause Indicates that the security policy name in the **secPolicyAdd** command does not exist.

Recommended action Create the appropriate security policy first, then use its name in the **secPolicyAdd** command to add new members.

Severity ERROR

SEC-1090

Message

```
<timestamp>, [SEC-1090], <sequence-number>,, ERROR,
<system-name>, SCC list contains FCS member. Please
remove member from the FCS policy first.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1091

Message

```
<timestamp>, [SEC-1091], <sequence-number>,, ERROR,
<system-name>, No policy to remove.
```

Probable cause Indicates that the specified policy member does not exist or the policy itself does not exist.

Recommended action Verify that the security policy name or member ID is correct.

Severity ERROR

SEC-1092

Message

```
<timestamp>, [SEC-1092], <sequence-number>,, ERROR,
<system-name>, <Policy name> Name not found.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1093

Message

```
<timestamp>, [SEC-1093], <sequence-number>,, ERROR,
<system-name>, New FCS list must have at least one member
in common with current FCS list.
```

Probable cause Indicates that the new fabric configurations server (FCS) list does not have a common member with the existing FCS list.

Recommended action Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

Severity ERROR

SEC-1094

Message

```
<timestamp>, [SEC-1094], <sequence-number>,, ERROR,
<system-name>, Policy member not found.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1095

Message `<timestamp>, [SEC-1095], <sequence-number>,, ERROR, <system-name>, Deleting FCS policy is not allowed.`

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1096

Message `<timestamp>, [SEC-1096], <sequence-number>,, ERROR, <system-name>, Failed to delete <policy name> because <reason text>`

Probable cause Indicates that a policy cannot be removed because deleting it would result in invalid security policy configuration.

Recommended action Verify the security policy configuration requirements and remove any policies that require the policy you want to remove first.

Severity ERROR

SEC-1097

Message `<timestamp>, [SEC-1097], <sequence-number>,, ERROR, <system-name>, Cannot find <active or defined> policy set.`

Probable cause Indicates that the specified policy could not be found.

Recommended action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1098

Message `<timestamp>, [SEC-1098], <sequence-number>,, ERROR, <system-name>, No <active or defined> FCS list.`

Probable cause Indicates that the specified policy could not be found.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1099

Message `<timestamp>, [SEC-1099], <sequence-number>,, ERROR, <system-name>, Please enable your switch before running secModeEnable.`

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1100

Message `<timestamp>, [SEC-1100], <sequence-number>,, ERROR, <system-name>, FCS switch present. Command terminated.`

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1101

Message

```
<timestamp>, [SEC-1101], <sequence-number>,, ERROR,
<system-name>, Failed to enable security on all switches.
Please retry later.
```

Probable cause Indicates that the security enable failed on the fabric because one or more switches in the fabric are busy.

Recommended action Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity ERROR

SEC-1102

Message

```
<timestamp>, [SEC-1102], <sequence-number>,, ERROR,
<system-name>, Fail to download <security data>.
```

Probable cause Indicates that the switch failed to download certificate, security database, or policies. This can happen when switch does not get enough resources to complete the operation, fabric has not stabilized, or policy database is an invalid format.

Recommended action Wait for fabric to become stable and then retry the operation. If the policy database is in an illegal format (with **configDownload**), correct the format and retry the operation.

Severity ERROR

SEC-1104

Message `<timestamp>, [SEC-1104], <sequence-number>,, ERROR, <system-name>, Fail to get primary <Certificate or public key>.`

Probable cause Indicates that the switch failed to get either the primary certificate or a primary public key.

Recommended action Verify that the primary switch has a valid certificate installed and retry the operation.

Severity ERROR

SEC-1105

Message `<timestamp>, [SEC-1105], <sequence-number>,, ERROR, <system-name>, Fail to disable secure mode on all switches.`

Probable cause Indicates that the switch failed to disable security in the fabric. This could happen if the switch cannot get the required resources to complete the command, and sending to a remote domain fails or the remote domain returns an error.

Recommended action Run the **secFabricShow** to verify that all switches in the fabric are in the ready state. Retry the command when all switches are READY.

Severity ERROR

SEC-1106

Message `<timestamp>, [SEC-1106], <sequence-number>,, ERROR, <system-name>, Failed to sign message data.`

Probable cause Indicates that some public key infrastructure (PKI) objects on the switch are not in a valid state, and a signature operation failed.

Recommended action Run the **pkiShow** command and verify that all PKI objects exist on the switch.

Severity ERROR

SEC-1107

Message

```
<timestamp>, [SEC-1107], <sequence-number>,, INFO,
<system-name>, Stamp is 0.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1108

Message

```
<timestamp>, [SEC-1108], <sequence-number>,, ERROR,
<system-name>, Fail to reset stamp on all switches.
```

Probable cause Indicates that a version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

Recommended action Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity ERROR

SEC-1110

Message

```
<timestamp>, [SEC-1110], <sequence-number>,, ERROR,
<system-name>, FCS list must be the first entry in the
[Defined Security policies] section. Fail to download
defined database.
```

Probable cause Indicates that a security policy download is attempted with a defined policy that does not have the fabric configurations server (FCS) policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

Recommended action Download a correct configuration with the FCS policy as the first policy in the defined security database.

Severity ERROR

SEC-1111

Message

```
<timestamp>, [SEC-1111], <sequence-number>,, ERROR,
<system-name>, New defined FCS list must have at least
one member in common with current active FCS list. Fail
to download defined database.
```

Probable cause Indicates that the defined and active fabric configurations server (FCS) policy list failed to have at least one member in common.

Recommended action A new FCS policy list must have at least one member in common with the previous FCS policy.

Severity ERROR

SEC-1112

Message

```
<timestamp>, [SEC-1112], <sequence-number>,, ERROR,
<system-name>, FCS list must be the first entry in the
Active Security policies, and the same as the current
active FCS list in the switch.
```

Probable cause Indicates that either a security policy download is attempted with an active policy that does not have the fabric configurations server (FCS) policy as the first policy or the FCS policy is not same as the current FCS policy on the switch.

Recommended action Make sure that the new FCS policy is the same as the current FCS policy on the switch.

Severity ERROR

SEC-1113

Message `<timestamp>, [SEC-1113], <sequence-number>,, WARNING, <system-name>, <Key> [ <Feature> license ] going to expire in <Expiry_days> day(s).`

Probable Cause Indicates that the license period will expire soon.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-1114

Message `<timestamp>, [SEC-1114], <sequence-number>,, WARNING, <system-name>, <Key> [ <Feature> license ] is expired.`

Probable Cause Indicates that the license period has expired.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-1115

Message `<timestamp>, [SEC-1115], <sequence-number>,, ERROR, <system-name>, No primary FCS to failover.`

Probable cause Indicates that during an attempted **secFcsFailover**, no primary fabric configurations server (FCS) is present in the fabric.

Recommended action Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity ERROR

SEC-1116

Message

```
<timestamp>, [SEC-1116], <sequence-number>,, ERROR,
<system-name>, Fail to commit failover.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

ERROR

SEC-1117

Message

```
<timestamp>, [SEC-1117], <sequence-number>,, INFO,
<system-name>, Fail to set <data>.
```

Probable cause

Indicates that the switch failed to save the data received by the primary fabric configurations server (FCS) switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

Recommended action

Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity

INFO

SEC-1118

Message

```
<timestamp>, [SEC-1118], <sequence-number>,, INFO,
<system-name>, Fail to set SNMP string.
```

Probable cause

Indicates that the SNMP string could not be set.

Recommended action Usually this problem is transient. Retry the command.

Severity INFO

SEC-1119

Message
```
<timestamp>, [SEC-1119], <sequence-number>,, INFO,
<system-name>, Secure mode has been enabled.
```

Probable cause Indicates that the secure Fabric OS was enabled by the **secModeEnable** command.

Recommended action Verify that the security event was planned. If the security event was planned, there is no action required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1121

Message
```
<timestamp>, [SEC-1121], <sequence-number>,, ERROR,
<system-name>, Time is out of range when <text>.
```

Probable cause Indicates that the time on the switch is not synchronized with the primary fabric configurations server (FCS), the data packet is corrupted, or a replay attack is launched on the switch.

Recommended action Verify that the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1122

Message
```
<timestamp>, [SEC-1122], <sequence-number>,, INFO,
<system-name>, Error code: <Domain ID>, <Error message>.
```

Probable cause Indicates that one of the switches in the fabric could not communicate with the primary fabric configurations server (FCS).

Recommended action Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity INFO

SEC-1123

Message `<timestamp>, [SEC-1123], <sequence-number>,, INFO, <system-name>, Security database downloaded by Primary FCS.`

Probable cause Indicates that the security database was successfully downloaded from the primary fabric configurations server (FCS).

Recommended action No action is required.

Severity INFO

SEC-1124

Message `<timestamp>, [SEC-1124], <sequence-number>,, INFO, <system-name>, Secure Mode is off.`

Probable cause Indicates that a secure mode disable is attempted in a non-secure fabric.

Recommended action No action is required.

Severity INFO

SEC-1126

Message `<timestamp>, [SEC-1126], <sequence-number>,, INFO, <system-name>, Secure mode has been disabled.`

Probable cause Indicates that a secure mode disable operation completed successfully.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1130

Message

```
<timestamp>, [SEC-1130], <sequence-number>,, INFO,
<system-name>, The Primary FCS has failed over to a new
switch.
```

Probable cause Indicates that an FCS failover operation was completed successfully.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1135

Message

```
<timestamp>, [SEC-1135], <sequence-number>,, INFO,
<system-name>, Secure fabric version stamp has been
reset.
```

Probable cause Indicates that the version stamp of the secure fabric is reset.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1136

Message

```
<timestamp>, [SEC-1136], <sequence-number>,, ERROR,
<system-name>, Failed to verify signature <data type,
MUA, policy, etc.,>.
```

Probable cause Indicates that the receiving switch fails to validate the security database sending from the primary fabric configurations server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity ERROR

SEC-1137

Message

```
<timestamp>, [SEC-1137], <sequence-number>,, ERROR,
<system-name>, No signature in <data type, MUA, policy,
etc.,>.
```

Probable cause Indicates that the receiving switch fails to validate the security database sending from the primary fabric configurations server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity ERROR

SEC-1138

Message

```
<timestamp>, [SEC-1138], <sequence-number>,, INFO,
<system-name>, Security database download received from
Primary FCS.
```

Probable cause

Indicates that a non-primary fabric configurations server (FCS) switch received a security database download.

Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1139

Message

```
<timestamp>, [SEC-1139], <sequence-number>,, ERROR,
<system-name>, The RSNMP_POLICY cannot exist without the
WSNMP_POLICY.
```

Probable cause

Indicates that the receiving switch fails to validate the security database sending from the primary fabric configurations server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity

ERROR

SEC-1142

Message

```
<timestamp>, [SEC-1142], <sequence-number>,, INFO,
<system-name>, Reject new policies. <reason text>.
```

Probable cause Indicates that the new polices are rejected due to the reason specified.

Recommended action Use proper syntax when entering policy information.

Severity INFO

SEC-1145

Message

```
<timestamp>, [SEC-1145], <sequence-number>,, INFO,
<system-name>, A security admin event has occurred. This
message is for information purpose only. The message for
individual event is: <Event specific data>
```

Probable cause Indicates one of the following has occurred:

- The names for the specified policies have changed.
- The passwords have changed for the specified accounts.
- The SNMP community strings have been changed.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1146

Message

```
<timestamp>, [SEC-1146], <sequence-number>,, INFO,
<system-name>, PID changed: <State>.
```

Probable cause Indicates that the PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the device connection control (DCC) polices existed, all index/area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an index/area of 127 before changing to extended-edge PID, then the new index/area is 15, because of the wraparound.

Recommended action No action is required.

Severity INFO

SEC-1153

Message

```
<timestamp>, [SEC-1153], <sequence-number>,, INFO,
<system-name>, Error in RCA: RCS is not supported
```

Probable cause

Indicates that reliable commit service (RCS) is not supported.

Recommended action

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

For any switch that does not support RCS, upgrade the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

INFO

SEC-1154

Message

```
<timestamp>, [SEC-1154], <sequence-number>,, INFO,
<system-name>, PID change failed: <Reason> <defined
status> <active status>.
```

Probable cause

Indicates that either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the index/area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended action

Reduce the size of the policy database.

Severity

INFO

SEC-1155

Message

```
<timestamp>, [SEC-1155], <sequence-number>,, INFO,
<system-name>, PID change failed: <Reason> <defined
status> <active status>.
```

Probable cause Indicates that either the defined or active policy was too large after modifying the index/area ID. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended action Reduce the size of the specified policy database.

Severity INFO

SEC-1156

Message

```
<timestamp>, [SEC-1156], <sequence-number>,, INFO,
<system-name>, Change failed: <Reason> <defined status>
<active status>.
```

Probable cause Indicates that the security daemon is busy. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended action For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands might take a few minutes to propagate throughout the fabric. Make sure to wait a few minutes between executing commands so that your commands do not overlap in the fabric.

Severity INFO

SEC-1157

Message

```
<timestamp>, [SEC-1157], <sequence-number>,, INFO,
<system-name>, PID Change failed: <Reason> <defined
status> <active status>.
```

Probable cause Indicates that the provisioning resources for a security policy failed due to low memory or internal error. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended action Retry the failed command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

SEC-1158

Message
```
<timestamp>, [SEC-1158], <sequence-number>,, INFO,
<system-name>, Invalid name <Policy or Switch name>.
```

Probable cause Indicates that the specified name is invalid. The name can be a policy name or a switch name.

Recommended action Enter a valid name.

Severity INFO

SEC-1159

Message
```
<timestamp>, [SEC-1159], <sequence-number>,, INFO,
<system-name>, Non_Reachable domain <Domain ID>.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1160

Message
```
<timestamp>, [SEC-1160], <sequence-number>,, INFO,
<system-name>, Duplicate port <port ID> in port list
(<port list>).
```

Probable cause Indicates that a duplicate port member exists in the specified port list.

Recommended action Verify that there is no duplicate member in the port list.

Severity INFO

SEC-1163

Message `<timestamp>, [SEC-1163], <sequence-number>,, ERROR, <system-name>, System is already in secure mode. Lockdown option cannot be applied.`

Probable cause Indicates that the lockdown option was attempted while the fabric is already in secure mode.

Recommended action Do not use the lockdown option with the **secModeEnable** command when switch is already in secure mode.

Severity ERROR

SEC-1164

Message `<timestamp>, [SEC-1164], <sequence-number>,, ERROR, <system-name>, Lockdown option cannot be applied on a non-FCS switch.`

Probable cause Indicates that the attempt to enable security is made on a switch that is not present in the fabric configurations server (FCS) list.

Recommended action Add the switch into the FCS policy list when using the lockdown option to enable security.

Severity ERROR

SEC-1165

Message `<timestamp>, [SEC-1165], <sequence-number>,, ERROR, <system-name>, Low memory, failed to enable security on all switches.`

Probable cause Indicates that the system is low on memory.

Recommended action Wait a few minutes and try the command again.

Severity ERROR

SEC-1166

Message `<timestamp>, [SEC-1166], <sequence-number>,, ERROR, <system-name>, Non FCS tries to commit failover.`

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1167

Message `<timestamp>, [SEC-1167], <sequence-number>,, ERROR, <system-name>, Another FCS failover is in process. Command terminated.`

Probable cause Indicates that because another failover is already in progress, this failover attempt cannot proceed.

Recommended action Verify that the security event was planned. If the security event was planned, retry fabric configurations server (FCS) failover after current failover has completed, if this switch should become primary FCS. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity ERROR

SEC-1168

Message `<timestamp>, [SEC-1168], <sequence-number>,, ERROR, <system-name>, Primary FCS failover is busy. Please retry later.`

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1170

Message

```
<timestamp>, [SEC-1170], <sequence-number>,, INFO,
<system-name>, This command must be executed on the
Primary FCS switch, the first reachable switch in the FCS
list.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1171

Message

```
<timestamp>, [SEC-1171], <sequence-number>,, ERROR,
<system-name>, Disabled secure mode due to invalid
security object.
```

Probable cause Indicates that the switch is segmented, and secure mode is disabled on the switch because there was no license present or no public key infrastructure (PKI) objects.

Recommended action Run the **pkiShow** command to check if all PKI objects exist. If they do not exit, run the **pkiCreate** command to create them for the switch.

Run the **licenseAdd** command to install the required license key.

Severity ERROR

SEC-1172

Message
```
<timestamp>, [SEC-1172], <sequence-number>,, ERROR,
<system-name>, Failed to identify role.
```

Probable cause Indicates that the switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

Recommended action Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1173

Message
```
<timestamp>, [SEC-1173], <sequence-number>,, ERROR,
<system-name>, Lost contact with Primary FCS switch.
```

Probable cause Indicates that the switch has lost contact with the primary fabric configurations server (FCS) switch in the secure fabric. This could be due to the primary FCS being disabled.

Recommended action If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

Severity ERROR

SEC-1174

Message
```
<timestamp>, [SEC-1174], <sequence-number>,, ERROR,
<system-name>, Failed to set <FCS or non-FCS> password.
```

Probable cause Indicates that the FCS or non-FCS password could not be set.

Recommended action Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1175

Message `<timestamp>, [SEC-1175], <sequence-number>,, ERROR, <system-name>, Failed to install zone data.`

Probable cause Indicates that the zone database could not be installed on the switch.

Recommended action Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1176

Message `<timestamp>, [SEC-1176], <sequence-number>,, ERROR, <system-name>, Failed to generate new version stamp.`

Probable cause Indicates that the primary fabric configurations server (FCS) failed to generate a new version stamp due to the fabric not being stable.

Recommended action Verify that all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1180

Message `<timestamp>, [SEC-1180], <sequence-number>,, INFO, <system-name>, Added account <user name> with <role name> authorization.`

Probable cause Indicates that the specified new account has been created.

Recommended action No action is required.

Severity INFO

SEC-1181

Message `<timestamp>, [SEC-1181], <sequence-number>,, INFO, <system-name>, Deleted account <user name>`

Probable cause Indicates that the specified account has been deleted.

Recommended action No action is required.

Severity INFO

SEC-1182

Message `<timestamp>, [SEC-1182], <sequence-number>,, INFO, <system-name>, Recovered <number of> accounts.`

Probable cause Indicates that the specified number of accounts have been recovered from backup.

Recommended action No action is required.

Severity INFO

SEC-1183

Message `<timestamp>, [SEC-1183], <sequence-number>,, ERROR, <system-name>, Policy to binary conversion error: Port <port number> is out range.`

Probable cause Indicates that a security database conversion has failed because of an invalid value.

Recommended action Retry the command with a valid value.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1184

Message

```
<timestamp>, [SEC-1184], <sequence-number>,, INFO,
<system-name>, <server> configuration change, action
<action>, server ID <server>
```

Probable cause Indicates that the specified action is applied to the specified remote authentication dial-in user service (RADIUS)/Lightweight Director Access Protocol (LPAD) server configuration. The possible values for *actions* are "ADD", "REMOVE", "CHANGE", and "MOVE".

Recommended action No action is required.

Severity INFO

SEC-1185

Message

```
<timestamp>, [SEC-1185], <sequence-number>,, INFO,
<system-name>, <action> switch DB.
```

Probable cause Indicates that the switch database was enabled or disabled as the secondary authentication, accounting, and authorization (AAA) mechanism when the remote authentication dial-in user service (RADIUS) / Lightweight Director Access Protocol (LPAD) is the primary AAA mechanism.

Recommended action No action is required.

Severity INFO

SEC-1186

Message

```
<timestamp>, [SEC-1186], <sequence-number>,, INFO,
<system-name>, <action> Configuration.
```

Probable cause Indicates that the remote authentication dial-in user service (RADIUS/LDAP) configuration was enabled or disabled as the primary authentication, accounting, and authorization (AAA) mechanism.

Recommended action No action is required.

Severity INFO

SEC-1187

Message

```
<timestamp>, [SEC-1187], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized switch
<switch WWN> tries to join fabric.
```

Probable cause Indicates that a switch connection control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended action Check the switch connection control policy (SCC) policy to verify the switches allowed in the fabric. If the switch should be allowed in the fabric but not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1188

Message

```
<timestamp>, [SEC-1188], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized device
<device node name> tries to FLOGI to index/area <port
number> of switch <switch WWN>.
```

Probable cause Indicates that a device connection control (DCC) security violation was reported. The specified device attempted to login using fabric login (FLOGI) to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes connected port, the device will not be allowed to login.

Recommended action Check the DCC policy and verify that the specified device is allowed in the fabric and is included in the DCC policy. If the specified device not included in the policy, add it to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1189

Message

```
<timestamp>, [SEC-1189], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address> tries to do SNMP write operation.
```

Probable cause Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

Recommended action Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1190

Message

```
<timestamp>, [SEC-1190], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address> tries to do SNMP read operation.
```

Probable cause Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation.

Recommended action Check the RSNMP policy to verify that hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized

entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1191

Message

```
<timestamp>, [SEC-1191], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <Ip address> tries to establish HTTP
connection.
```

Probable cause Indicates that an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended action Check if the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1192

Message

```
<timestamp>, [SEC-1192], <sequence-number>,, INFO,
<system-name>, Security violation: Login failure attempt
via <connection method>.
```

Probable cause Indicates that a serial or modem login security violation was reported. An incorrect password was used while trying to log in through a serial or modem connection; the login failed.

Recommended action Use the correct password.

Severity INFO

SEC-1193

Message

```
<timestamp>, [SEC-1193], <sequence-number>,, INFO,
<system-name>, Security violation: Login failure attempt
via <connection method>. IP Addr: <IP address>
```

Probable cause

Indicates that a specified login security violation was reported. The incorrect password was used while trying to log in through the specified connection method; the login failed.

Recommended action

The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

Severity

INFO

SEC-1194

Message

```
<timestamp>, [SEC-1194], <sequence-number>,, WARNING,
<system-name>, This switch does not have all the required
PKI objects correctly installed.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity

WARNING

SEC-1195

Message

```
<timestamp>, [SEC-1195], <sequence-number>,, WARNING,
<system-name>, This switch has no <component> license.
```

Probable cause

Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric

configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity WARNING

SEC-1196

Message `<timestamp>, [SEC-1196], <sequence-number>,, WARNING, <system-name>, Switch does not have all default account names.`

Probable cause Indicates that the default switch accounts admin and user do not exist on the switch when enabling security.

Recommended action Reset the default admin and user account names on the switch that reported the warning and retry enabling security.

Severity WARNING

SEC-1197

Message `<timestamp>, [SEC-1197], <sequence-number>,, INFO, <system-name>, Changed account <user name>.`

Probable cause Indicates that the specified account has changed.

Recommended action No action is required.

Severity INFO

SEC-1198

Message

```
<timestamp>, [SEC-1198], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized host with
IP address <IP address> tries to establish API
connection.
```

Probable cause

Indicates that an API security violation was reported. The specified unauthorized host attempted to establish an API connection.

Recommended action

Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1199

Message

```
<timestamp>, [SEC-1199], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized access to
serial port of switch <switch instance>.
```

Probable cause

Indicates that a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

Recommended action

Check to see if an authorized access attempt is being made on the console. If so, add the switch world-wide name (WWN) to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1200

Message

```
<timestamp>, [SEC-1200], <sequence-number>,, INFO,
<system-name>, Security violation: MS command is
forwarded from non-primary FCS switch.
```

Probable cause

Indicates that a management server (MS) forward security violation was reported. A management server command was forwarded from a non-primary fabric configurations server (FCS) switch.

Recommended action

Check the MS policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1201

Message

```
<timestamp>, [SEC-1201], <sequence-number>,, INFO,
<system-name>, Security violation: MS device <device WWN>
operates on non-primary FCS switch.
```

Probable cause

Indicates that a management server (MS) operation security violation was reported. An MS device operation occurred on a non-primary fabric configurations server (FCS) switch.

Recommended action

Check the management server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection is MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1202

Message

```
<timestamp>, [SEC-1202], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized access
from MS device node name <device node name>, device port
name <device port name>.
```

Probable cause

Indicates that a management server (MS) security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

Recommended action

Check the MS server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1203

Message

```
<timestamp>, [SEC-1203], <sequence-number>,, INFO,
<system-name>, Login information: Login successful via
TELNET/SSH/RSH. IP Addr: <IP address>
```

Probable cause

Indicates the IP address of the remote station logging in.

Recommended action

No action is required.

Severity

INFO

SEC-1250

Message

```
<timestamp>, [SEC-1250], <sequence-number>,, WARNING,
<system-name>, DCC enforcement API failed: <failed
action> err=<status>, key=<data>
```

Probable cause

Indicates that an internal error caused the DCC policy enforcement to fail.

Recommended action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

SEC-1251

Message

```
<timestamp>, [SEC-1251], <sequence-number>,, ERROR,
<system-name>, Policy to binary conversion error: <text
message> <value>.
```

Probable cause

Indicates that the security database conversion failed because of invalid values. The reason is specified in the *text message* variable and faulty value is printed in *value* variable.

Recommended action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

SEC-1253

Message

```
<timestamp>, [SEC-1253], <sequence-number>,, ERROR,
<system-name>, Bad DCC interface state during <Phase>,
state=<state>.
```

Probable cause

Indicates that an internal error has caused the device connection control (DCC) policy update to fail in the provision, commit, or cancel phases.

Recommended action

Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

SEC-1300

Message

```
<timestamp>, [SEC-1300], <sequence-number>,, INFO,
<system-name>, This switch is in VcEncode mode. Security
is not supported.
```

Probable cause Indicates that the switch is set up with VC-encoded mode.

Recommended action Turn off VC-encoded mode before enabling security.

Severity INFO

SEC-1301

Message

```
<timestamp>, [SEC-1301], <sequence-number>,, INFO,
<system-name>, This switch is in interop mode. Security
is not supported.
```

Probable cause Indicates that the switch is interop-mode enabled.

Recommended action Disable interop-mode using the **interopMode** command before enabling the Secure Fabric OS feature.

Severity INFO

SEC-1302

Message

```
<timestamp>, [SEC-1302], <sequence-number>,, INFO,
<system-name>, This switch does not have all the required
PKI objects correctly installed.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1303

Message

```
<timestamp>, [SEC-1303], <sequence-number>,, INFO,
<system-name>, This software version does not support
security.
```

Probable cause Indicates that the currently installed software version does not support the Secure Fabric OS feature.

Recommended action Run the **firmwareDownload** command to update the firmware to the latest version for your specific switch. Verify that the firmware you are installing supports the Secure Fabric OS feature.

Severity INFO

SEC-1304

Message

```
<timestamp>, [SEC-1304], <sequence-number>,, INFO,
<system-name>, This switch has no security license.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1305

Message

```
<timestamp>, [SEC-1305], <sequence-number>,, INFO,
<system-name>, This switch has no zoning license.
```

Probable cause Indicates that there has been a corruption during the distribution of the security database. This can only occur when the primary fabric

configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1306

Message

```
<timestamp>, [SEC-1306], <sequence-number>,, INFO,
<system-name>, Failed to verify certificate with root CA.
```

Probable cause Indicates that the certificate could not be verified with root certificate authority (CA). This could happen if an unauthorized switch tries to access the fabric that is not certified by a trusted root CA or a root CA certificate does not exist on the switch.

Recommended action Run the **pkiShow** command and verify that all public key infrastructure (PKI) objects exist on the switch. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

Severity INFO

SEC-1307

Message

```
<timestamp>, [SEC-1307], <sequence-number>,, INFO,
<system-name>, Got response from <Radius/LPAD server
identity> server <Radius/LPAD server identity>.
```

Probable cause Indicates that after some servers timed out, the specified remote authentication dial-in user service (RADIUS/LPAD) server responded to a switch request.

Recommended action If the message appears frequently, move the responding server to the top of the RADIUS/LPAD server configuration list using the **aaaConfig** command.

Severity INFO

SEC-1308

Message

```
<timestamp>, [SEC-1308], <sequence-number>,, INFO,
<system-name>, All RADIUS servers have failed to respond.
```

Probable cause

Indicates that all servers in the remote authentication dial-in user service (RADIUS) configuration have failed to respond to a switch request within the specified time-out.

Recommended action

Verify that the switch has proper network connectivity to the specified remote authentication dial-in user service (RADIUS) servers, and the servers are correctly configured.

Severity

INFO

SEC-1309

Message

```
<timestamp>, [SEC-1309], <sequence-number>,, INFO,
<system-name>, Waiting for RCS transaction to complete:
<Wait time in seconds> secs
```

Probable cause

Indicates that Secure Fabric OS is still waiting for the reliable commit service (RCS) transaction to complete.

Recommended action

Verify if there are any RCS or RTWR errors. If not, the transaction is still in progress.

Severity

INFO

SEC-1310

Message

```
<timestamp>, [SEC-1310], <sequence-number>,, INFO,
<system-name>, Unable to determine data distribution
limit of fabric. Please retry later.
```

Probable cause

Unable to obtain the data distribution limit from all switches in the fabric. This may happen if the fabric is reconfiguring or a new domain joined the fabric.

Recommended action

Retry the command when the fabric is stable.

Severity

INFO

SEC-1311

Message

```
<timestamp>, [SEC-1311], <sequence-number>,, ERROR,
<system-name>, Security mode cannot be enabled because
one or more of the password policies is not set to
default value.
```

Probable cause

Indicates that the security enable failed on the fabric because one or more switches in the fabric have password policies that are not set to the default value.

Recommended action

Verify that the security event was planned.

If the security event was planned, run the **passwdCfg --setDefault** command on each switch in the fabric to set the password policies to the default value. Then verify with **passwdCfg --show** that password policies are set to the default values on all switches and retry the **secModeEnable** command.

Severity

ERROR

SEC-1312

Message

```
<timestamp>, [SEC-1312], <sequence-number>,, INFO,
<system-name>, <MESG Message>.
```

Probable cause

Indicates that the **passwdCfg** parameters changed.

Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1313

Message

```
<timestamp>, [SEC-1313], <sequence-number>,, INFO,
<system-name>, The passwdcfg parameters were set to
default values.
```

Probable cause

Indicates that the **passwdCfg** parameters were set to default values.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1314

Message

```
<timestamp>, [SEC-1314], <sequence-number>,, ERROR,
<system-name>, Reading <IP Address Description > IP
address from EM failed.
```

Probable cause Indicates that the call to the EM module to retrieve the IP address failed.

Recommended action Reboot the system to fix this error. If the problem persists, run **supportFTP** (as needed) to set up automatic FIP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1315

Message

```
<timestamp>, [SEC-1315], <sequence-number>,, ERROR,
<system-name>, <Name of command > command failed -<List
of databases rejecting distribution > db(s) configured
for rejection on this switch
```

Probable cause Attempt to distribute database(s) to a switch that was configured not to accept distributions from the fabric.

Recommended action Verify the accept distribution configuration for the listed databases. Use the **fddCfg** command to verify and correct the configuration if necessary.

Severity ERROR

SEC-1316

Message `<timestamp>, [SEC-1316], <sequence-number>,, WARNING, <system-name>, <Policy Name> policy is conflicting with domain <Domain Number>`

Probable cause Indicates that the newly added switches to the fabric, as specified by *Domain Number,* have a conflicting policy with the local switch.

Recommended action Check the conflicting policy and make the new switches and the local switch policies the same.

Severity WARNING

SEC-1317

Message `<timestamp>, [SEC-1317], <sequence-number>,, INFO, <system-name>, Inconsistent fabric, rejecting transaction`

Probable cause Indicates that either this domain is performing an FDD merge or matched domains are not the same as what the CM sees.

Recommended action If a policy conflict exists, resolve it, then wait for the fabric to become stable. Retry the distribution.

Severity INFO

SEC-1318

Message `<timestamp>, [SEC-1318], <sequence-number>,, INFO, <system-name>, Transaction rejected due to inconsistent fabric`

Probable cause Indicates that some domains detected an inconsistent fabric.

Recommended action Resolve policy conflict, if there is one, then wait for the fabric to stabilize. Retry the distribution.

Severity INFO

SEC-1319

Message

```
<timestamp>, [SEC-1319], <sequence-number>,, INFO,
<system-name>, <Event name> updated <Datasets updated>
dbs(s)
```

Probable cause

Indicates that the specified event has occurred.

Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-1320

Message

```
<timestamp>, [SEC-1320], <sequence-number>,, WARNING,
<system-name>, Non-acl domain <Domain Number> tries to
join a fabric with strict fabric wide policy
```

Probable cause

Indicates that a domain not supporting an access control list (ACL) policy tried to join a fabric with a strict fabric-wide policy.

Recommended action

No action is required. The domain is denied by disallowing all its E_Ports from connecting to the fabric.

Severity

WARNING

SEC-1321

Message

```
<timestamp>, [SEC-1321], <sequence-number>,, ERROR,
<system-name>, Failed secure mode enable command. Reason:
<Reason>.
```

Probable cause

Indicates that the security enable failed on the fabric because switch has conflicting configuration such as fabric wide consistency configuration or AD configuration.

Recommended action

Verify that the security event was planned.

If the security event was planned, run the **fddcfg --fabwideset ""** command or **ad --clear** command to clear the fabric wide

consistency configuration or AD configuration and retry the **secModeEnable** command.

Severity ERROR

SEC-1322

Message `<timestamp>, [SEC-1322], <sequence-number>,, WARNING, <system-name>, Some DCC policy is too large, distribution cancelled`

Probable cause Indicates that this fabric is not able to support a device connection control (DCC) policy with more than 256 ports.

Recommended action Reconfigure any policy that includes more than 256 ports in its member list, then save the policy configuration changes.

Severity WARNING

SEC-1323

Message `<timestamp>, [SEC-1323], <sequence-number>,, INFO, <system-name>, Key(s) \"<Key Name>\" ignored during configdownload.`

Probable cause Indicates that the specified key is ignored during **configDownload**.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1324

Message `<timestamp>, [SEC-1324], <sequence-number>,, INFO, <system-name>, Fabric transaction failure. RCS error: <Error code>`

Probable cause Indicates that the reliable commit service (RCS) transaction failed with specified reason code.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1325

Message

```
<timestamp>, [SEC-1325], <sequence-number>,, ERROR,
<system-name>, Security enforcement: Switch <switch WWN>
connecting to port <Port number> is not authorized to
stay in fabric.
```

Probable cause Indicates that due to a switch connection control (SCC) policy violation, the switch is being disabled on the specified port.

Recommended action No action is required unless the switch must remain in the fabric. If the switch must remain in the fabric, add the switch world-wide name (WWN) to the SCC policy, then attempt to join the switch with the fabric.

Severity ERROR

SEC-1326

Message

```
<timestamp>, [SEC-1326], <sequence-number>,, INFO,
<system-name>, Event: fddcfg --fabwideset, Status:
success, Info: Fabric wide configuration set to
<Fabric-wide configuration set by user>.
```

Probable cause Indicates that the specified event has occurred.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1327

Message `<timestamp>, [SEC-1327], <sequence-number>,, WARNING, <system-name>, Strict <Policy Name> policy is conflicting with domain <Domain Number>`

Probable cause Strict policy is conflicting.

Recommended action None, the domain is denied by disallowing all its E-ports connected to the fabric. If the domain should be allowed to merge with the fabric, then resolve the issue by making the conflicting policies same.

Severity WARNING

SEC-1328

Message `<timestamp>, [SEC-1328], <sequence-number>,, ERROR, <system-name>, Attempt to enable secure mode failed. Reason: <Reason>.`

Probable cause Indicates that the **secModeEnable** command failed on the fabric, because Authentication Policy is enabled on the switch.

Recommended action Verify that the security event was planned. If the security event was planned, run the **authUtil --policy passive** command to disable the Authentication Policy and retry the **secModeEnable** command.

Severity ERROR

SEC-1329

Message `<timestamp>, [SEC-1329], <sequence-number>,, ERROR, <system-name>, IPFilter enforcement: Failed to enforce ipfilter policy of <policy Type> type because of <Error code>.`

Probable cause Indicates that the IP filter policy enforcement failed due to internal system failure.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SEC-1330

Message

```
<timestamp>, [SEC-1330], <sequence-number>,, ERROR,
<system-nam>, <Name of command> command failed - <List of
databases rejecting distribution> db(s) are coming from a
non-Primary switch.
```

Probable cause Indicates that an attempt was made to distribute database(s) either from a backup fabric configuration server (FCS) switch or from a non-FCS switch.

Recommended action Verify that the distribution is initiated by the primary FCS switch. Use the **secPolicyShow** command to verify and correct the configuration if necessary.

Severity ERROR

SEC-1331

Message

```
<timestamp>, [SEC-1331], <sequence-number>,, ERROR,
<system-name>, Attempt to enable secure mode failed.
Reason: <Reason>.
```

Probable Cause Indicates the **secModeEnable** command failed on the fabric because default IP Filter policies are not active on the switch, or an active transaction exists on IP Filter policies.

Recommended Action Verify the security event was planned. If the security event was planned, run the **ipfilter --activate default_ipv4** or the **ipfilter --activate default_ipv6** command to activate default IP Filter Policies. Use the **ipfilter --save** or the **ipfilter --transabort** commands to save or abort any active transaction on IP Filter policies. Then retry the **secModeEnable** command.

Severity ERROR

SEC-1332

Message

```
<timestamp>, [SEC-1332], <sequence-number>,, ERROR,
<system-name>, Fabric wide policy is conflicting as
<Policy Name> is present in the fabric wide policy and
5.3 or 5.2 switches present in the fabric.
```

Probable Cause Policy is conflicting.

Recommended Action Remove either FCS from fabric wide policy or 5.3 and 5.2 switches from the fabric, or set the fabric wide mode for FCS as Strict.

Severity ERROR

SEC-1333

Message

```
<timestamp>, [SEC-1333], <sequence-number>,, ERROR,
<system-name>, <Name of command> command failed. There
are VF enabled switches in fabric. <List of databases
rejecting distribution> db(s) distribution is blocked.
```

Probable Cause Indicates there was an attempt to distribute PWD/IPFILTER databases from the fabric to a switch that is Virtual Fabrics-enabled.

Recommended Action Disable Virtual Fabrics on all the switches that have it enabled if PWD/ IPFILTER databases need to be distributed.

Severity ERROR

SEC-3035

Message

```
<timestamp>, [SEC-3035], <sequence-number>, AUDIT, INFO,
<system-name>, Event: ipfilter, Status: success, Info:
<IP Filter Policy> ipfilter policy(ies) saved.
```

Probable Cause Indicates that the specified IP filter policy has been saved.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3036

Message `<timestamp>, [SEC-3036], <sequence-number>, AUDIT, INFO, <system-name>, Event: ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy> ipfilter policy(s).`

Probable Cause Indicates that that the specified IP filter policy has not been saved.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3037

Message `<timestamp>, [SEC-3037], <sequence-number>, AUDIT, INFO, <system-name>, Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.`

Probable Cause Indicates that that the specified IP filter policy has been activated.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3038

Message `<timestamp>, [SEC-3038], <sequence-number>, AUDIT, INFO, <system-name>, Event: ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter policy.`

Probable Cause Indicates that the specified IP filter policy failed to activate.

Recommended Action Verify that the security event was planned. If the event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3039

Message

```
<timestamp>, [SEC-3039], <sequence-number>, AUDIT, INFO,
<system-name>, Event:Securty Violation , Status: failed,
Info: Unauthorized host with IP address <IP address of
the violating host> tries to establish connection using
<Protocol Connection Type>.
```

Probable Cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the specified protocol connection.

Severity INFO

SEC-3050

Message

```
<timestamp>, [SEC-3050], <sequence-number>, AUDIT, INFO,
<system-name>, Event: <Event Name>, Status: success,
Info: <Event Specific Info>.
```

Probable Cause Indicates that the specified sshutil operation was performed.

Recommended Action Verify if the security event was planned, if yes then no action is required else take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3051

Message

```
<timestamp>, [SEC-3051], <sequence-number>, AUDIT, INFO,
<system-name>, The license key <key> is <Action>.
```

Probable Cause Indicates that a license key is added or removed.

Recommended Action No action is required.

Severity INFO

75

SNMP System Messages

This chapter contains information on the following SNMP messages:

- SNMP-1001 716
- SNMP-1002 716
- SNMP-1003 716
- SNMP-1004 717
- SNMP-1005 717
- SNMP-1006 717
- SNMP-1007 718
- SNMP-1008 718

SNMP-1001

Message

```
<timestamp>, [SNMP-1001], <sequence-number>,, ERROR,
<system-name>, SNMP service is not available <Reason>.
```

Probable cause

Indicates that the simple network management protocol (SNMP) service could not be started because of the specified *Reason*. You will not be able to query the switch through SNMP.

Recommended action

Verify that the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified *Reason* is an initialization failure, the switch requires a reboot.

Severity

ERROR

SNMP-1002

Message

```
<timestamp>, [SNMP-1002], <sequence-number>,, ERROR,
<system-name>, SNMP <Error Details> initialization
failed.
```

Probable cause

Indicates that the initialization of the simple network management protocol (SNMP) service failed and you will not be able to query the switch through SNMP.

Recommended action

Reboot or power cycle the switch. This automatically initializes SNMP.

Severity

ERROR

SNMP-1003

Message

```
<timestamp>, [SNMP-1003], <sequence-number>,, ERROR,
<system-name>, Distribution of Community Strings to
Secure Fabric failed.
```

Probable cause

Indicates that the changes in the simple network management protocol (SNMP) community strings could not be propagated to other switches in the secure fabric.

Recommended action

Retry changing the SNMP community strings from thee primary switch.

Severity ERROR

SNMP-1004

Message `<timestamp>, [SNMP-1004], <sequence-number>, FFDC, ERROR, <system-name>, Incorrect SNMP configuration.`

Probable cause Indicates that the simple network management protocol (SNMP) configuration is incorrect and the SNMP service will not work correctly.

Recommended action Change the SNMP configuration back to the default.

Severity ERROR

SNMP-1005

Message `<timestamp>, [SNMP-1005], <sequence-number>, AUDIT, INFO, <system-name>, SNMP configuration attribute, <Changed attribute>, has changed from <Old Value> to <New Value>`

Probable cause Indicates that the simple network management protocol (SNMP) configuration has changed. The parameter that was modified is displayed as well as the old and new values for that parameter.

Recommended action Execute the **snmpConfig --show** command to see the new configuration.

Severity INFO

SNMP-1006

Message `<timestamp>, [SNMP-1006], <sequence-number>, AUDIT, INFO, <system-name>, <SNMP Configuration group> configuration was reset to default`

Probable cause Indicates that the simple network management protocol (SNMP) configuration group was reset to the factory default.

Recommended action Execute the **snmpConfig --show** command for the group to see the new configuration.

Severity INFO

SNMP-1007

Message

```
<timestamp>, [SNMP-1007], <sequence-number>,, INFO,
<system-name>, The last fabric change happened at:
<string>.
```

Probable Cause Indicates the last fabric change time.

Recommended Action Execute the **fabricshow** command to view the current fabric status.

Severity INFO

SNMP-1008

Message

```
<timestamp>, [SNMP-1008], <sequence-number>,, INFO,
<system-name>, The last device change happened at:
<string>.
```

Probable Cause Indicates the last device change time.

Recommended Action Execute the **nsshow** command to view the current device status.

Severity INFO

76

SPC System Messages

This chapter contains information on the following SPC messages:

- SPC-1001 721
- SPC-1002 721
- SPC-1003 721
- SPC-2002 722
- SPC-2003 722
- SPC-2004 723
- SPC-2005 723
- SPC-2006 723
- SPC-2007 724
- SPC-2008 724
- SPC-2009 724
- SPC-2010 725
- SPC-2011 725
- SPC-2012 725
- SPC-3001 726
- SPC-3002 726
- SPC-3003 726
- SPC-3004 727
- SPC-3005 727
- SPC-3006 728
- SPC-3007 728
- SPC-3008 729
- SPC-3009 729
- SPC-3010 730
- SPC-3011 730
- SPC-3012 730
- SPC-3013 731

- SPC-3014 731
- SPC-3015 732

SPC-1001

Message `<timestamp>, [SPC-1001], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, Cryptographic operation enabled.`

Probable Cause Indicates the cryptographic operation is enabled on an encryption engine.

Recommended Action No action is required.

Severity INFO

SPC-1002

Message `<timestamp>, [SPC-1002], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, Cryptographic operation disabled.`

Probable Cause Indicates the cryptographic operation is disabled on an encryption engine.

Recommended Action No action is required.

Severity INFO

SPC-1003

Message `<timestamp>, [SPC-1002], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, Security Processor faulted.`

Probable Cause Indicates the security processor is faulted because of an internal error. Cryptographic operations are affected.

Recommended Action For a bladed system, perform **slotpoweroff** and **slotpoweron** commands on the blade to recover the system. For a non-bladed system, perform a **fastboot** command on the switch to recover the system.

Severity INFO

SPC-2001

Message

```
<timestamp>, [SPC-2001], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Crypto error asserted by
Vader/OB1 0x%x.
```

Probable Cause Indicates the Crypto error asserted by FPGA.

Recommended Action No action is required.

Severity INFO

SPC-2002

Message

```
<timestamp>, [SPC-2002], <sequence-number>,, CRITICAL,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Tamper Event: Crypto subsystem
cover tampered.
```

Probable Cause Indicates the Crypto subsystem cover has been tampered with. The Encryption Engine (EE) has been zeroized.

Recommended Action Run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to re-initialize and register the EE.

Severity CRITICAL

SPC-2003

Message

```
<timestamp>, [SPC-2003], <sequence-number>,, INFO,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Data Disable status: 0x%x.
```

Probable Cause Indicates the Data disable signal status.

Recommended Action No action is required.

Severity INFO

SPC-2004

Message `<timestamp>, [SPC-2004], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: FPGA firmware download failed: 0x%x.`

Probable Cause Indicates the FPGA download failed.

Recommended Action No action is required.

Severity INFO

SPC-2005

Message `<timestamp>, [SPC-2005], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: FPGA firmware download success: 0x%x.`

Probable Cause Indicates the FPGA download was successful.

Recommended Action No action is required.

Severity INFO

SPC-2006

Message `<timestamp>, [SPC-2006], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: Crypto post tests failed: 0x%x.`

Probable Cause Indicates the Crypto POST tests failed.

Recommended Action No action is required.

Severity INFO

SPC-2007

Message

```
<timestamp>, [SPC-2007], <sequence-number>,, INFO,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Crypto post tests success: 0x%x.
```

Probable Cause Indicates the Crypto POST tests passed successfully.

Recommended Action No action is required.

Severity INFO

SPC-2008

Message

```
<timestamp>, [SPC-2008], <sequence-number>,, INFO,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Vader/OB1 recovered from error.
```

Probable Cause Indicates the Crypto error from FPGA de-asserted.

Recommended Action No action is required.

Severity INFO

SPC-2009

Message

```
<timestamp>, [SPC-2009], <sequence-number>,, CRITICAL,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Tamper event:  User zeroization.
```

Probable Cause Indicates the Tamper event triggered due to a user initiated zeroize request. The Encryption Engine (EE) has been zeroized.

Recommended Action Run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to re-initialize and register the EE.

Severity CRITICAL

SPC-2010

Message

```
<timestamp>, [SPC-2010], <sequence-number>,, CRITICAL,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Crypto subsystem cover is open.
```

Probable Cause Indicates the Crypto subsystem cover is open.

Recommended Action Close the crypto subsystem cover properly.

Severity CRITICAL

SPC-2011

Message

```
<timestamp>, [SPC-2011], <sequence-number>,, INFO,
<system-name>, <slot number containing Encryption
Engine>, <module name>: OB1 crypto BIST success.
```

Probable Cause Indicates the FPGA BIST was successful.

Recommended Action No action is required.

Severity INFO

SPC-2012

Message

```
<timestamp>, [SPC-2012], <sequence-number>,, INFO,
<system-name>, <slot number containing Encryption
Engine>, <module name>: User zeroization command
completed successfully. Tamper INT status %x.
```

Probable Cause Indicates the user initiated zeroization command completed successfully. The encryption engine (EE) has been zeroized.

Recommended Action Run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to re-initialize and register the EE.

Severity INFO

SPC-3001

Message

<timestamp>, [SPC-3001], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No input KEK for DEK inject, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.

Probable Cause

Indicates the wrapping Key Encryption Key (KEK) for the Data Encryption Key (DEK) to be injected does not exist within the Encryption Engine (EE) Crypto Module.

Recommended Action

For opaque key vaults such as RKM, recover the missing Master Key to current or alternate position.

Severity

ERROR

SPC-3002

Message

<timestamp>, [SPC-3002], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No input KEK for DEK rewrap, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.

Probable Cause

Indicates the input wrapping Key Encryption Key (KEK) for the Data Encryption Key (DEK) to be rewrapped does not exist within the EE Crypto Module.

Recommended Action

For opaque key vaults such as RKM, recover the missing Master Key to the current or alternate position.

Severity

ERROR

SPC-3003

Message

<timestamp>, [SPC-3003], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No output KEK for DEK rewrap, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.

Probable Cause Indicates the output wrapping Key Encryption Key (KEK) for the Data Encryption Key (DEK) to be rewrapped does not exist within the Encryption Engine Crypto Module.

Recommended Action No action is required. The KEK will be recovered automatically.

Severity ERRORData Encryption Key (DEK)

SPC-3004

Message

```
<timestamp>, [SPC-3004], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: No output KEK for DEK create,
KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet
4>.
```

Probable Cause Indicates the output wrapping Key Encryption Key (KEK) for the Data Encryption Key (DEK) to be created does not exist within the EE Crypto Module.

Recommended Action For opaque key vaults such as RKM, recover the missing Master Key to the current or alternate position.

Severity ERROR

SPC-3005

Message

```
<timestamp>, [SPC-3005], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>:DEK inject error: <SP status
code>, DEK: <DEK octet 1 or other info> <DEK octet 2>
<DEK octet 3> <DEK octet 4>.
```

Probable Cause Cause is determined by the value of *SP status* code.

- 14 - Attempt to inject a Data Encryption Key (DEK) to an invalid FPGA table index
- 14 - Invalid input DEK format
- 32 - DEK could not be unwrapped
- 33 - FGPA error upon inject
- 73 - Invalid Key Encryption Key (KEK) format

Recommended Action Run **supportFTP** (as needed) to set up automatic FIP transfers; then run the supportSave command and contact the EMC Customer Support Center.

Severity ERROR

SPC-3006

Message

```
<timestamp>, [SPC-3006], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>:DEK rewrap error: <SP status
code>, DEK: <DEK octet 1 or other info> <DEK octet 2>
<DEK octet 3> <DEK octet 4>.
```

Probable Cause Cause is determined by the value of *SP status code*:

- 2 - Invalid input Data Encryption Key (DEK) format
- 14 - Rewrapping not allowed: primary Key Encryption Key (KEK) generation is in progress
- 31 - DEK could not be wrapped
- 32 - DEK could not be unwrapped
- 33 - FGPA error upon inject
- 73 - Invalid KEK format

Recommended Action For status code 14, complete the primary KEK generation; otherwise, run supportFTP (as needed) to set up automatic FIP transfers; then run the **supportSave command** and contact the EMC Customer Support Center.

Severity ERROR

SPC-3007

Message

```
<timestamp>, [SPC-3007], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: DEK create error: <SP status
code>, info: <other info>.
```

Probable Cause Cause is determined by the value of *SP status code*:

- 2 - Invalid input Data Encryption Key (DEK) specification
- 21 - No primary Key (KEK) exists with which to wrap the DEK

- 14 - Creation not allowed: primary KEK generation is in progress
- 31 - DEK could not be wrapped
- 73 - Invalid KEK format
- other - Internal error

Recommended Action For status code 14, complete the primary KEK generation; otherwise run **supportFTP** (as needed) to set up automatic FIP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SPC-3008

Message

```
<timestamp>, [SPC-3008], <sequence-number>,, INFO,
<system-name>, <slot number containing Encryption
Engine>, <module name>: SP crypto got READY notification.
```

Probable Cause Indicates the key application (KPD) within the Crypto Module of the Encryption Engine (EE) has been started.

Recommended Action No action is required.

Severity INFO

SPC-3009

Message

```
<timestamp>, [SPC-3009], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: FIPS certificate mismatch,
certificate: <FIPS certificate is CO-0 or User-1>.
```

Probable Cause Indicates the FIPS certificate within the Crypto Module does not match that of the node.

Recommended Action Run the **cryptoCfg --zeroizeEE** command to zeroize the Encryption Engine (EE) (after backing up any needed primary or secondary Key Encryption Key (KEK), then run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to re-initialize and register the EE.

Severity ERROR

SPC-3010

Message

```
<timestamp>, [SPC-3010], <sequence-number>,, WARNING,
<system-name>, <slot number containing Encryption
Engine>, <module name>: SEK integrity failure during
initialization.
```

Probable Cause Indicates the Crypto Module internal Secret Encryption Key has been corrupted or has not been initialized.

Recommended Action Run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to initialize and register the EE.

Severity ERROR

SPC-3011

Message

```
<timestamp>, [SPC-3011], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Persistent data storage error:
<SP status code>, KEK: <KEK octet 1> <KEK octet 2> <KEK
octet 3> <KEK octet 4>.
```

Probable Cause Indicates an attempt to store Crypto Module internal data using the Secret Encryption Key failed - most likely, the Encryption Engine (EE) has been zeroized or tampered with.

Recommended Action Run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to initialize and register the EE. then recover or restore the needed primary and secondary Key Encryption Keys (KEKs).

Severity ERROR

SPC-3012

Message

```
<timestamp>, [SPC-3012], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: Persistent data retrieval error:
<SP status code>.
```

Probable Cause Indicates an attempt to read Crypto Module internal data using the Secret Encryption Key failed - most likely, the Encryption Engine (EE) has been zeroized or tampered with.

Recommended Action Run the **cryptoCfg --initEE** and **cryptoCfg --regEE** commands to re-initialize and register the EE, then recover or restore the needed primary and secondary Key Encryption Keys (KEKs).

Severity ERROR

SPC-3013

Message

```
<timestamp>, [SPC-3013], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: SEK generation failure: <SP
status code>.
```

Probable Cause Indicates the Crypto Module internal Secret Encryption Key could not be generated.

Recommended Action Run **supportFTP** (as needed) to set up automatic FIP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SPC-3014

Message

```
<timestamp>, [SPC-3014], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: RNG compare failure: successive
values match.
```

Probable Cause Indicates the Crypto Module internal random number generator failed.

Recommended Action Run **supportFTP** (as needed) to set up automatic FIP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

SPC-3015

Message

```
<timestamp>, [SPC-3015], <sequence-number>,, ERROR,
<system-name>, <slot number containing Encryption
Engine>, <module name>: RSA pairwise key generation test
failure.
```

Probable Cause

Indicates the Crypto Module could not generate its internal key pair.

Recommended Action

Run **supportFTP** (as needed) to set up automatic FIP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

77

SPM System Messages

This chapter contains information on the following SPM messages:

- SPM-1001 734
- SPM-1002 734
- SPM-1003 734
- SPM-1004 734
- SPM-1005 735
- SPM-1006 735
- SPM-1007 735
- SPM-1008 736
- SPM-1009 736
- SPM-1010 736

SPM-1001

Message `<timestamp>, [SPM-1001], <sequence-number>,, ERROR, <system-name>, Init fails: <Reason>.`

Probable Cause Indicates SPM failed to initialize.

Recommended Action Check system resources and reboot switch.

Severity ERROR

SPM-1002

Message `<timestamp>, [SPM-1002], <sequence-number>,, WARNING, <system-name>, Generic SPM Warning: <Reason>.`

Probable Cause Identified by the *reason*.

Recommended Action Run **supportFTP** (as needed) to set up automatic FIP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

SPM-1003

Message `<timestamp>, [SPM-1003], <sequence-number>,, INFO, <system-name>, Set New Group Cfg SC Enable <SC_Enable> KV Type <KV_Type>.`

Probable Cause A new encryption group has been configured.

Recommended Action No action is required.

Severity INFO

SPM-1004

Message `<timestamp>, [SPM-1004], <sequence-number>,, INFO, <system-name>, Initialize Node.`

Probable Cause A node has been initialized.

Recommended Action No action is required.

Severity INFO

SPM-1005

Message

```
<timestamp>, [SPM-1005], <sequence-number>,, INFO,
<system-name>, Set EE Control slot <slot> action
<action>.
```

Probable Cause The *action* has been performed on the Encryption Engine in *slot*.

Recommended Action No action is required.

Severity INFO

SPM-1006

Message

```
<timestamp>, [SPM-1006], <sequence-number>,, INFO,
<system-name>, Registered Certificate of type
<cert_type>.
```

Probable Cause A certificate of *type* has been registered with the Encryption Engine (EE).

Recommended Action No action is required.

Severity INFO

SPM-1007

Message

```
<timestamp>, [SPM-1007], <sequence-number>,, INFO,
<system-name>, Deregistered Certificate cid [<cert_id>]
type <cert_type> idx <qc_idx>.
```

Probable Cause A certificate of *type* has been registered with the Encryption Engine (EE).

Recommended Action No action is required.

Severity INFO

SPM-1008

Message
```
<timestamp>, [SPM-1008], <sequence-number>,, INFO,
<system-name>, Deregistered SP Certificate in slot
<slot>.
```

Probable Cause A node SP certificate has been deregistered for the Encryption Engine (EE) in *slot*.

Recommended Action No action is required.

Severity INFO

SPM-1009

Message
```
<timestamp>, [SPM-1009], <sequence-number>,, ERROR,
<system-name>, <cert> Certificate is missing.
```

Probable Cause A certificate of type *cert* is missing.

Recommended Action Run **cryptocfg --initnode** command to initialize the node and generate the equired certificates.

Severity ERROR

SPM-1010

Message
```
<timestamp>, [SPM-1010], <sequence-number>,, ERROR,
<system-name>, <cert> Key Vault Certificate is missing.
```

Probable Cause A required certificate is missing for the Key Vault.

Recommended Action Run the c**ryptoCfg --dereg -keyvault** and **cryptoCfg --reg -keyvault** commands to deregister and register this key vault.

Severity ERROR

78

SS System Messages

This chapter contains information on the following SS messages:

- SS-1000 740
- SS-1001 740
- SS-1002 741
- SS-1003 741

SS-1000

Message

```
<timestamp>, [SS-1000], <sequence-number>,, INFO,
<system-name>, supportSave has ftp'ed support information
to the host with IP address <host ip>.
```

Probable cause

Indicates that the **supportSave** command was used to transfer support information to a remote FTP location.

Recommended action

No action is required.

Severity

INFO

SS-1001

Message

```
<timestamp>, [SS-1001], <sequence-number>,, WARNING,
<system-name>, supportSave's upload operation to host IP
address <host ip> aborted.
```

Probable cause

Indicates that a file copy error occurred during execution of the **supportSave** command. Complete error information cannot always be displayed in this message due to possible errors in subcommands being executed by the **supportSave** command.

Recommended action

Check the remote server and settings. Run the **supportFtp** command to set the FTP or SCP parameters. After the FTP problem is corrected, rerun the **supportSave** command.

Severity

WARNING

SS-1002

Message

```
<timestamp>, [SS-1002], <sequence-number>,, INFO,
<system-name>, supportSave has stored support information
to the USB storage device.
```

Probable Cause

Indicates that the **supportSave** command was used to transfer support information to an attached USB storage device.

Recommended Action

No action is required.

Severity

INFO

SS-1003

Message

```
<timestamp>, [SS-1003], <sequence-number>,, WARNING,
<system-name>, supportSave's operation to USB storage
device aborted.
```

Probable Cause

Indicates that a USB operation error occurred during execution of the **supportSave** command. Complete error information cannot always be displayed in this message due to possible errors in subcommands being executed by the **supportSave** command.

Recommended Action

Run **usbstorage** to check the USB storage device settings. After the USB problem is corrected, rerun the **supportSave** command.

Severity

WARNING

79

SULB System Messages

This chapter contains information on the following SULB messages:

- SULB-1001 745
- SULB-1002 745
- SULB-1003 745
- SULB-1004 746
- SULB-1005 746
- SULB-1006 746
- SULB-1007 747
- SULB-1008 747
- SULB-1009 747
- SULB-1010 756
- SULB-1011 756
- SULB-1017 757
- SULB-1018 757
- SULB-1020 757
- SULB-1021 758
- SULB-1022 758
- SULB-1023 759
- SULB-1024 759
- SULB-1025 760
- SULB-1026 760
- SULB-1030 760
- SULB-1031 761
- SULB-1032 761
- SULB-1033 761
- SULB-1034 762
- SULB-1035 762
- SULB-1036 762

◆ SULB-1037 763

SULB-1001

Message

```
<timestamp>, [SULB-1001], <sequence-number>, AUDIT,
WARNING, <system-name>, Firmwaredownload command has
started.
```

Probable cause

Indicates that the **firmwareDownload** command has been entered. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended action

Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption. Do not fail over or power down the system during firmware upgrade. No action is required.

Run the **firmwareDownloadStatus** command for more information.

Severity

WARNING

SULB-1002

Message

```
<timestamp>, [SULB-1002],<sequence-number>, AUDIT, INFO,
<system-name>, Firmwaredownload command has completed
successfully.
```

Probable cause

Indicates that the **firmwareDownload** command has completed successfully and switch firmware has been updated.

Recommended action

No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information. Run **firmwareShow** to verify the firmware versions.

Severity

INFO

SULB-1003

Message

```
<timestamp>, [SULB-1003], <sequence-number>, AUDIT, INFO,
<system-name>, Firmwarecommit has started.
```

Probable cause

Indicates that the **firmwareCommit** command has been entered.

Recommended action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1004

Message

```
<timestamp>, [SULB-1004], INFO, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwarecommit has completed.
```

Probable Cause Indicates that the **FirmwareCommit** command is executed.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1005

Message

```
<timestamp>, [SULB-1005], <sequence-number>,, INFO,
<system-name>, Current Active CP is preparing to
failover.
```

Probable cause Indicates that the active CP is about to reboot. The standby CP is taking over as the active CP.

Recommended action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1006

Message

```
<timestamp>, [SULB-1006], <sequence-number>,, INFO,
<system-name>, Forced failover succeeded. New Active CP
is running new firmware.
```

Probable cause Indicates that the previous standby has now become the active CP and is running the new firmware version.

Recommended action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1007

Message `<timestamp>, [SULB-1007], <sequence-number>,, INFO, <system-name>, Standby CP reboots.`

Probable cause Indicates that the standby CP is rebooting with new firmware.

Recommended action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1008

Message `<timestamp>, [SULB-1008], <sequence-number>,, INFO, <system-name>, Standby CP booted successfully with new firmware.`

Probable cause Indicates that the standby CP has rebooted successfully.

Recommended action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1009

Message `AUDIT, <timestamp>, [SULB-1009], AUDIT, INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload command failed. status: 0x<status code>, error: 0x<error code>.`

Probable cause Indicates that the **firmwareDownload** command failed. The additional *status code* and *error code* provide debugging information.

Table 6 lists **firmwareDownload** status messages and status codes. Some of them will not show up in this RASLOG message. They are listed for the sake of completeness.

Table 6 Status messages and status codes (1 of 4)

Status message	Status code
"**firmwareDownload** sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because **firmwareDownload** is already in progress."	0x32
"Sanity check failed because FABRIC OS is disabled on Active CP."	0x33
"Sanity check failed because HAMD is disabled on Active CP."	0x34
"Sanity check failed because **firmwareDownload** is already in progress."	0x35
"Sanity check failed because FABRIC OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
"**firmwareDownload** failed on Standby CP."	0x40
"**firmwareDownload** failed on Standby CP."	0x41
"**firmwareDownload** failed on Standby CP."	0x42
"**firmwareCommit** failed on Standby CP."	0x43
"**firmwareDownload** failed."	0x44
"**firmwareDownload** failed due to IPC error."	0x50
"Unable to check the firmware version on Standby CP due to IPC error."	0x51
"**firmwareDownload** failed due to IPC error."	0x52
"**firmwareDownload** failed due to IPC error."	0x53
"Standby CP failed to reboot due to IPC error."	0x54
"**firmwareCommit** operation failed due to IPC error."	0x55
"Unable to check the firmware version on Standby CP due to IPC error."	0x56
"Unable to restore the original firmware due to Standby CP timeout."	0x57

Table 6 Status messages and status codes (2 of 4)

Status message	Status code
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on Standby CP due to IPC error."	0x59
“Sanity check failed because **firmwareDownload** is already in progress.”	0x60
“Sanity check failed because **firmwareDownload** is already in progress.”	0x61
NOT USED	0x62
"System Error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Active and Standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
“**firmwareCommit** has started to restore the secondary partition.”	0x69
"Local CP is restoring its secondary partition."	0x6a
“Unable to restore the secondary partition. Please use **firmwareDownloadStatus** and **firmwareShow** to see firmware status.”	0x6b
“**firmwareDownload** has started on Standby CP. It might take up to 10 minutes.”	0x6c
“**firmwareDownload** has completed successfully on Standby CP.”	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
“**firmwareDownload** has completed successfully on Standby CP.”	0x72
“**firmwareDownload** has started on Standby CP. It might take up to 10 minutes.”	0x73
“**firmwareDownload** has completed successfully on Standby CP.”	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76

Table 6 Status messages and status codes (3 of 4)

Status message	Status code
“**firmwareCommit** has started on Standby CP.”	0x77
“**firmwareCommit** has completed successfully on Standby CP.”	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
“**firmwareCommit** has started on both Active and Standby CPs.”	0x7b
“**firmwareCommit** has completed successfully on both CPs.”	0x7c
“**firmwareCommit** failed on Active CP.”	0x7d
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
“There was an unexpected reboot during **firmwareDownload**. The command is aborted.”	0x84
"Standby CP was not responding. The command is aborted."	0x85
“**firmwareCommit** has started on both CPs. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x86
“**firmwareCommit** has started on the local CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x87
“**firmwareCommit** has started on the remote CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x88
“Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x89
“**firmwareDownload** command has completed successfully.”	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e

Table 6 Status messages and status codes (4 of 4)

Status message	Status code
“**firmwareDownload** has started.”	0x8f
“**firmwareCommit** has started.”	0x90
“**firmwareDownload** has completed successfully.”	0x91
“**firmwareCommit** has completed successfully.”	0x92
“**firmwareCommit** has started to restore the secondary partition.”	0x93
“**firmwareCommit** failed.”	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
“**firmwareDownload** timed out.”	0xa1
“Reboot occurred during **firmwareDownload**. **firmwareCommit** will be started to recover the blade.”	0xa2
“Blade rebooted during **firmwareCommit**. The operation will be restarted.”	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5
“New firmware failed to boot up. Please retry **firmwareDownload**.”	0xa6
“**firmwareCommit** has started on the blade. This may take up to 10 minutes.”	0xa7
“**firmwareRestore** is entered. System will reboot and a **firmwareCommit** operation will start upon boot up.”	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
“Blade failed to reboot with the original image. **firmwareRestore** command failed.”	0xac

Table 7 lists additional **firmwareDownload** error messages and error codes. They provide more details on why **firmwareDownload** failed.

Table 7 Error messages and error codes (1 of 2)

Error message	Error code
"Image is up-to-date. No need to download the same version of firmware."	0xF
“Upgrade is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x10
“OSRootPartition is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding. For example: swap OSRootPartitions and reboot.”	0x11
“Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check **firmwareDownload** help page for other possible failure reasons.”	0x12
"The RPM package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
“Error in getting lock device for **firmwareDownload**.”	0x18
“Error in releasing lock device for **firmwareDownload**.”	0x19
“**firmwareCommit** failed.”	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
“OSLoader is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x1d
“New image has not been committed. Run **firmwareCommit** or **firmwareRestore** first and then try **firmwareDownload**.”	0x1e
“**firmwareRestore** failed.”	0x1f
"Both images are mounted to the same device."	0x20
“Unable to unionist old packages.”	0x21
“**firmwareDownload** is already in progress.”	0x22

Table 7 Error messages and error codes (2 of 2)

Error message	Error code
“**firmwareDownload** timed out.”	0x23
"Our of disk space."	0x24
“Primary filesystem is inconsistent. Run **firmwareRestore** to restore the original firmware, or contact your service provider for recovery.”	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Please contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
“The platform option is not supported. Run **chassisConfig** to reset the option first and then try **firmwareDownload**.”	0x2a
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version first and then download the desired version."	0x2c
“Cannot download 5.1 because Device Based Routing policy is not supported by 5.1. Use **aptPolicy** to change the routing policy before proceeding.”	0x2d
"Invalid RPM package. Please reload firmware packages on the file server."	0x2e
"Cannot downgrade due to presence of blade type 17. Remove or power off these blades before proceeding."	0x2f
"Cannot downgrade due to presence of blade type 24. Remove or power off these blades before "	0x30
"Cannot downgrade due to presence of long-distance ports in LS mode. Please remove these settings before proceeding."	0x31
"Network is not reachable. Please verify the IP address of the server is correct."	0x32

The following section explains the causes of some common error messages:

0x15 - Failed to download Red Hat package manager (RPM) package. If this error occurs immediately after **firmwareDownload** is started, the firmware on the switch may be two releases older than the requested firmware. **firmwareDownload** supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number, for example, X.Y). The following are major upgrade versions for the Fabric OS: v4.0, v4.1,

v4.2, v4.4, v5.0, v5.1.,5.2, and 5.3. In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of **firmwareDownload**, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmwareDownload** command. If the problem persists, contact your system administrator.

0x18 - Error in getting lock device for **firmwareDownload**. This error may occur because another **firmwareDownload** is already in progress. Run **firmwareDownloadStatus** to verify that this is the case. Wait for the current session to finish before proceeding.

0x23 - **firmwareDownload** timed out. This error may occur because **firmwareDownload** has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.

0x24 - out of disk space. This error may occur because some coredump files have not been removed from the filesystem and are using up disk space. Remove these coredump files using the **supportSave** command before proceeding.

0x29 - The pre-install script failed. This error may be caused by an unsupported blade type in the chassis. Remove or power off the unsupported blades before proceeding. Another possible cause may be an invalid **chassisConfig** option setting. In that case, reset the **chassisConfig** option before retrying **firmwareDownload**.

0x2e - Invalid Red Hat package manager (RPM) package. This error maybe caused by an inconsistent firmware image loaded on the file server. It may also be caused by temporary networking issues. Please reload firmware packages on the file server, then retry **firmwareDownload**. If the problem persists, contact your system administrator.

Table 8 lists the **firmwareDownload** state names and state values. They indicate where in the **firmwareDownload** process the error occurred.

Table 8 Upgrade state and code value (1 of 2)

Upgrade state	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23

Table 8 **Upgrade state and code value (2 of 2)**

Upgrade state	Code
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended action

Run the **firmwareDownloadStatus** command for more information.

In a director-class switch, when **firmwareDownload** fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another **firmwareDownload**.

In a director-class switch, when **firmwareDownload** fails, the two CPs may end up with different versions of firmware and they may not gain high-availability (HA) sync. In that case, run **firmwareDownload** single mode (**-s**) to upgrade the firmware on the

standby CP to the same version as the active CP. Then retry **firmwareDownload** to download the desired version of firmware onto the CPs.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for troubleshooting information.

Severity INFO

SULB-1010

Message `<timestamp>, [SULB-1010], <sequence-number>, AUDIT, INFO, <system-name>, Firmwarecommit failed (status=0x<error code>).`

Probable cause Indicates that the **firmwareCommit** failed. The error code provides debugging information. See Table 7 on page 752 for more information.

Recommended action If the failure is caused by an inconsistent filesystem, contact the EMC Customer Support Center.

Severity INFO

SULB-1011

Message `<timestamp>, [SULB-1011], <sequence-number>,, INFO, <system-name>, Firmwaredownload command failed. state: 0x<state code>, status: 0x<status code>.`

Probable cause Indicates that the **firmwareDownload** command failed. The additional *state code* indicates where in the process it failed. *Status code* provides debugging information (see the tables in message 1109).

Recommended action Run the **firmwareDownloadStatus** command for more information.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for troubleshooting information.

Severity INFO

SULB-1017

Message

```
<timestamp>, [SULB-1017], <sequence-number>, AUDIT,
ERROR, <system-name>, Firmwaredownload failed in slot
<Slot number>.
```

Probable cause

Indicates that **firmwareDownload** failed in the specified blade. The error may be caused by an inconsistent AP blade firmware stored on the active CP. It may also caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended action

Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload**. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact the EMC Customer Support Center.

Severity

ERROR

SULB-1018

Message

```
<timestamp>, [SULB-1018], <sequence-number>, AUDIT,
ERROR, <system-name>, Firmwaredownload timed out in slot
<Slot number>.
```

Probable cause

The error may be caused by a blade initialization issue after the new firmware is downloaded and the blade is rebooted. The error may also be caused by an internal Ethernet issue or by a persistent storage failure.

Recommended action

Run the **slotShow** command. If the blade is in FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload**. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact the EMC Customer Support Center.

Severity

ERROR

SULB-1020

Message

```
<timestamp>, [SULB-1020], AUDIT, ERROR, <system-name>,
New firmware failed to boot in slot <Slot number>.
```

Probable cause The BP blade should reboot with the new image, but is still running the old image. This error may indicate that the new image has not been loaded correctly to the specified blade.

Recommended action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload** to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact the EMC Customer Support Center.

Severity ERROR

SULB-1021

Message

```
<timestamp>, [SULB-1021],<sequence-number>, AUDIT,
WARNING, <system-name>, Firmware is being downloaded to
the blade in slot <Slot number>.
```

Probable cause Indicates that the firmware is being loaded to the indicated blade.

Recommended action Run the **firmwareDownloadStatus** command to monitor the **firmwareDownload** progress. After it finishes, run the **firmwareShow** command to verify the firmware versions.

Severity WARNING

SULB-1022

Message

```
<timestamp>, [SULB-1022], <sequence-number>,, WARNING,
<system-name>, The blade in slot <Slot number> has
rebooted successfully with new firmware.
```

Probable cause Indicates that the blade in the specified slot has rebooted with new firmware. This is a normal step in the **firmwareDownload** process.

Recommended action Run the **firmwareDownloadStatus** command to monitor the **firmwareDownload** progress.

Severity WARNING

SULB-1023

Message

```
<timestamp>, [SULB-1023], AUDIT, WARNING, <system-name>,
The blade in slot <Slot number> has rebooted during
firmwaredownload.
```

Probable cause

The error may be caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering off and on of the indicated BP blade in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended action

firmwareCommit will be started automatically after the blade boots up to repair the secondary partition. If at the end of **firmwareCommit**, the blade firmware version is still inconsistent with the active CP firmware, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact the EMC Customer Support Center.

Severity

WARNING

SULB-1024

Message

```
<timestamp>, [SULB-1024], AUDIT, WARNING, <system-name>,
Firmware commit has completed on the blade in slot <Slot
number>.
```

Probable cause

Indicates that the **firmwareCommit** operation has completed on the specified blade.

Recommended action

Run the **firmwareShow** command to verify the firmware versions. If the blade firmware is the same as the active CP firmware, **firmwareDownload** has completed successfully on the blade. However, if the **firmwareCommit** operation has been started to repair the secondary partition, at the end of **firmwareCommit**, the blade firmware version may still be inconsistent with the active CP firmware. In that case, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress.

Severity

WARNING

SULB-1025

Message

```
<timestamp>, [SULB-1025], <sequence-number>,, WARNING,
<system-name>, The blade in slot <Slot number> will
reboot with the new firmware.
```

Probable cause

Indicates that new firmware has been downloaded to the specified AP blade and that the AP blade will reboot to active it.

Recommended action

Wait for the blade to reboot.

Severity

WARNING

SULB-1026

Message

```
<timestamp>, [SULB-1026], <sequence-number>, AUDIT,
WARNING, <system-name>, Firmware commit operation started
on the blade in slot <Slot number>.
```

Probable cause

firmwareCommit has started on the specified blade. The operation may be a normal part of **firmwareDownload**, or it may have started to repair the secondary partition of the blade if the secondary partition is corrupted.

Recommended action

No action is required.

Severity

WARNING

SULB-1030

Message

```
<timestamp>, [SULB-1030], AUDIT, WARNING, <system-name>,
The switch has rebooted during relocating the internal
firmware image.
```

Probable cause

The error may be caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering the switch off and on in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended action **firmwareDownload** will continue after the switch has rebooted. Run the **firmwareDownloadStatus** command to monitor progress. If the problem persists, contact the EMC Customer Support Center.

Severity WARNING

SULB-1031

Message

```
<timestamp>, [SULB-1031], <sequence-number>, AUDIT,
WARNING, <system-name>, The switch is relocating an
internal firmware image.
```

Probable cause Indicates that the switch has rebooted with the new firmware and is relocating the AP firmware.

Recommended action Wait for the operation to complete.

Severity WARNING

SULB-1032

Message

```
<timestamp>, [SULB-1032], <sequence-number>, AUDIT,
WARNING, <system-name>, Relocating an internal firmware
image on the CP.
```

Probable Cause Indicates the switch has started a firmware download to the co-CPU.

Recommended Action Wait for the operation to complete.

Severity WARNING

SULB-1033

Message

```
<timestamp>, [SULB-1033], <sequence-number>, AUDIT,
WARNING, <system-name>, Switch has completed relocating
the internal firmware image.
```

Probable cause Indicates that the **firmwareDownload** process has completed normally on the switch.

Recommended action Run the **firmwareShow** command to verify the firmware versions. Run the **switchShow** command to make sure the switch is enabled.

Severity WARNING

SULB-1034

Message

```
<timestamp>, [SULB-1034], <sequence-number>, AUDIT,
ERROR, <system-name>, Firmwaredownload timed out.
```

Probable cause The error may be caused by a switch initialization issue after the internal image is relocated. It may also be caused by an internal Ethernet issue or by persistent storage failure.

Recommended action Reboot the switch. This will cause the internal image to be relocated again. Use the **firmwareDownloadStatus** to monitor the progress. If the problem persists, contact the EMC Customer Support Center.

Severity ERROR

SULB-1035

Message

```
<timestamp>, [SULB-1035], <sequence-number>, AUDIT,
ERROR, <system-name>, An error has occurred during
relocation of the internal image.
```

Probable cause Indicates that an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by the internal Ethernet or persistent storage hardware failure.

Recommended action Reset the switch. This will cause the internal image to be relocated again. If the problem persists, contact the EMC Customer Support Center.

Severity ERROR

SULB-1036

Message

```
<timestamp>, [SULB-1036], <sequence-number>,, INFO,
<system-name>, <The Version being logged><Version String>
```

Probable cause Indicates the firmware version running in the system. This is generally logged before download and after download of the firmware to store version information.

Recommended action No action is required.

Severity INFO

SULB-1037

Message

```
<timestamp>, [SULB-1037], <sequence-number>, AUDIT, INFO,
<system-name>, HCL failed. Reboot the switch manually
using the reboot command. However, it will disrupt the FC
traffic.
```

Probable cause Many reasons can cause HCL to fail, such as domain not confirmed

Recommended action Run the **reBoot** command to reboot the switch manually.

Severity Error

80

SWCH System Messages

This chapter contains information on the following SWCH messages:

- SWCH-1001 766
- SWCH-1002 766
- SWCH-1003 766
- SWCH-1004 767
- SWCH-1005 767
- SWCH-1006 768
- SWCH-1007 768
- SWCH-1008 769
- SWCH-1009 769
- SWCH-1010 770
- SWCH-1011 770

SWCH-1001

Message

```
<timestamp>, [SWCH-1001], <sequence-number>,, ERROR,
<system-name>, Switch is not in ready state - Switch
enable failed switch status= 0x<switch status>, c_flags =
0x<switch control flags>.
```

Probable cause

Indicates that the switch is enabled before it is ready.

Recommended action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

SWCH-1002

Message

```
<timestamp>, [SWCH-1002], <sequence-number>,, INFO,
<system-name>, Security violation: Unauthorized device
<wwn name of device> tries to flogin to port <port
number>.
```

Probable cause

Indicates that the device is not present in the authorized profile list.

Recommended action

Verify that the device is authorized to log in to the switch. If the device is authorized, run the **secPolicyDump** command to verify whether the specified device world-wide name (WWN) is listed. If it is not listed, run the **secPolicyAdd** command to add this device to an existing policy.

Severity

INFO

SWCH-1003

Message

```
<timestamp>, [SWCH-1003], <sequence-number>,, ERROR,
<system-name>, Slot ENABLED but Not Ready during
recovery, disabling slot = <slot number>(<return value>).
```

Probable cause

Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended action On enterprise-class platforms, run the **slotPowerOff** command and then the **slotPowerOn** command.

On all others, reboot or power cycle the switch.

Severity ERROR

SWCH-1004

Message

```
<timestamp>, [SWCH-1004], <sequence-number>,, ERROR,
<system-name>, Blade attach failed during recovery,
disabling slot = <slot number>.
```

Probable cause Indicates that a blade has failed during failover or recovery.

Recommended action On enterprise-class platforms, run the **slotPowerOff** command and then the **slotPowerOn** command.

On all others, reboot or power cycle the switch.

Severity ERROR

SWCH-1005

Message

```
<timestamp>, [SWCH-1005], <sequence-number>,, ERROR,
<system-name>, Diag attach failed during recovery,
disabling slot = <slot number>.
```

Probable cause Indicates that the Diag blade attach has failed during failover or recovery.

Recommended action On enterprise-class platforms switch, run the **slotPowerOff** command and then the **slotPowerOn** command.

On all others, reboot or power cycle the switch.

Severity ERROR

SWCH-1006

Message

```
<timestamp>, [SWCH-1006], <sequence-number>,, WARNING,
<system-name>, HA state out of sync: Standby CP (ver =
<standby SWC version>) does not support NPIV
functionality. (active ver = <active SWC version>, NPIV
devices = <'1' if NPIV devices exist; Otherwise '0'. >).
```

Probable cause

Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality and the switch has some NPIV devices logged into the fabric.

Recommended action

Run the **firmwareDownload** command to load a firmware version on the standby CP that supports NPIV functionality.

Severity

WARNING

SWCH-1007

Message

```
<timestamp>, [SWCH-1007], <sequence-number>,, WARNING,
<system-name>, Switch port <port number> disabled due to
\"<disable reason>\".
```

Probable cause

Indicates that the switch port is disabled due to the reason displayed in the message.

Recommended action

Based on the disable reason displayed, proper corrective action may to be required to restore the port.

If insufficient frame buffers is the disable reason, reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link.

Please refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information about buffers.

Severity

WARNING

SWCH-1008

Message

```
<timestamp>, [SWCH-1008], <sequence-number>,, WARNING,
<system-name>, <area string> are port swapped on ports
that do not support port swap. Slot <slot number> will be
faulted.
```

Probable cause

Indicates that the blade is enabled with the port configuration that already has area swapped.

Recommended action

Replace the blade with ports that support port swap. Then port swap the ports back to ports default area.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information on port swapping.

Severity

WARNING

SWCH-1009

Message

```
<timestamp>, [SWCH-1009], <sequence-number>,, WARNING,
<system-name>, Shared area having Trunk Area (TA) enabled
on slot <slot number>. Shared areas that have TA enabled
will be persistenly disabled.
```

Probable Cause

The blade is enabled with a port configuration that had Trunk Area enabled on shared area port previously.

Recommended Action

Disable Trunk Area on ports that had Trunk Area enabled previously.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information.

Severity

WARNING

SWCH-1010

Message

```
<timestamp>, [SWCH-1010], <sequence-number>,, WARNING,
<system-name>, Trunk Area (TA) enabled on slot <slot
number> with switch not in PID format 1.  TA enabled
ports will be persistently disabled.
```

Probable Cause

The blade is enabled with the port configuration that had Trunk Area enabled previously.

Recommended Action

Disable Trunk Area on ports that had Trunk Area enabled previously.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for more information.

Severity

WARNING

SWCH-1011

Message

```
<timestamp>, [SWCH-1011], <sequence-number>,, WARNING,
<system-name>, HA state out of sync: Standby CP (ver =
<standby SWC version>) does not support Trunk Area
functionality. (active ver = <active SWC version>, Trunk
Area enabled on switch = <'1' if Trunk Area ports exist;
Otherwise '0'>).
```

Probable Cause

Indicates that the standby control processor (CP) does not support Trunk Area functionality, but the switch has some ports with Trunk Area enabled.

Recommended Action

Load a firmware version on standby that supports Trunk Area functionality, using the **firmwareDownload** command.

Severity

WARNING

81

SYSC System Messages

This chapter contains information on the following SYSC messages:

- SYSC-1001 772
- SYSC-1002 772
- SYSC-1003 773
- SYSC-1004 773
- SYSC-1005 774

SYSC-1001

Message

```
<timestamp>, [SYSC-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, Failed to run <Name of program
that could not be run (string)>:<System internal error
message (string)>.
```

Probable cause

Indicates that during the boot sequence, one of the programs would not run on the system.

Recommended action

If the message is reported during a reboot after new firmware has been loaded, try reloading the firmware using the **firmwareDownload** command.

If the message persists, there might be a conflict between the two versions of firmware or the nonvolatile storage might be corrupted. Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

SYSC-1002

Message

```
<timestamp>, [SYSC-1002], <sequence-number>, FFDC,
CRITICAL, <system-name>, Switch bring-up timed out.
```

Probable cause

Indicates that the system timed out during a reboot or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended action

The switch is in an inconsistent state and can be corrected only by a reboot or power cycle. Before rebooting the chassis, record the firmware version on the switch or control processor (CP) and run the **haDump** command. If this is a dual-CP switch, then gather the output from the CP in which this log message appeared.

Severity

CRITICAL

SYSC-1003

Message

```
<timestamp>, [SYSC-1003], <sequence-number>, FFDC,
CRITICAL, <system-name>, Chassis config option <Option
number read from the chassis option storage device> is
not supported by CP Blade with ID <Blade ID (platform)
number from the Active CP>. Change the chassis
configuration <Steps to change chassis configuration>
```

Probable cause

Indicates that on system startup, the option configuration file corresponding to the **chassisConfig** option read could not be found. This indicates that option is not supported on this platform running this version of the firmware.

It could also indicate that the current option number could not be read from the chassis option storage device (the world-wide name (WWN) card).

This message occurs only on the ED-48000B.

Recommended action

As indicated in the message, run the **chassisConfig** command to change to one that is valid on this platform running this firmware. Note that the **chassisConfig** option 1 should be valid for all platforms running any valid firmware.

Severity

CRITICAL

SYSC-1004

Message

```
<timestamp>, [SYSC-1004], <sequence-number>,, INFO,
<system-name>, Daemon <Daemon name to restart> restart
successful
```

Probable cause

Indicates that a terminated daemon is restarted by system automatically.

Recommended action

Use the **supportSave** command to gather troubleshooting data. No further action is required.

Severity

INFO

SYSC-1005

Message

```
<timestamp>, [SYSC-1005], <sequence-number>,, WARNING,
<system-name>, Daemon <Daemon name to restart> is not
restarted (Reason: <Restart failure reason>)
```

Probable cause

Indicates that a terminated daemon is not restarted, either due to restart limit is reached or restart action fails.

Recommended action

Use the **supportSave** command to gather troubleshooting data. Issue a **reboot** or **haFailover** command to recover the system and limit the traffic disruption.

Severity

WARNING

82

SYSM System Messages

This chapter contains information on the following SYSM messages:

- SYSM-1001 776
- SYSM-1002 776
- SYSM-1003 776
- SYSM-1004 777
- SYSM-1005 777
- SYSM-1006 777
- SYSM-1007 778

SYSM-1001

Message

```
<timestamp>, [SYSM-1001], <sequence-number>, FFDC,
CRITICAL, <system-name>, No memory.
```

Probable cause

Indicates that the switch has run out of system memory.

Recommended action

Run the **memShow** command to view the switch memory usage.

Reboot or power cycle the switch.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

CRITICAL

SYSM-1002

Message

```
<timestamp>, [SYSM-1002], <sequence-number>,, INFO,
<system-name>, <number>, Switch: <Switch number>
```

Probable cause

Indicates that a user has executed either the **switchShutdown** or **switchReboot** command. All services are brought down for a logical switch.

Recommended action

No action is required if the **switchShutdown** or **switchReboot** command was executed intentionally. If the **switchShutdown** command was run, you must run the **switchStart** command to restart traffic on the logical switch.

Severity

INFO

SYSM-1003

Message

```
<timestamp>, [SYSM-1003], <sequence-number>,, INFO,
<system-name>, <number>, Switch: <start reason>
```

Probable cause

Indicates that the user executed the **switchStart** or **switchReboot** command. This indicates that all services are brought back up after a temporary shutdown of that logical switch.

Recommended action No action is required if the **switchStart** command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity INFO

SYSM-1004

Message

```
<timestamp>, [SYSM-1004], <sequence-number>,, ERROR,
<system-name>, Failed to retrieve current chassis
configuration option, ret=<Unknown>
```

Probable cause Indicates that there was a failure to read configuration data from the WWN card.

Recommended action Verify that the world-wide name (WWN) card is present and operational and that the affected control processor (CP) is properly seated in its slot.

Severity ERROR

SYSM-1005

Message

```
<timestamp>, [SYSM-1005], <sequence-number>, FFDC,
CRITICAL, <system-name>, CP blade in slot <Slot number>
failed to retrieve current chassis type.
```

Probable cause Indicates that there was a failure to read the chassis type from the system.

Recommended action Verify that the control processor (CP) blade is operational and is properly seated in its slot.

Severity CRITICAL

SYSM-1006

Message

```
<timestamp>, [SYSM-1006], <sequence-number>, FFDC,
CRITICAL, <system-name>, CP blade in slot <Slot number>
is incompatible with the chassis type.
```

Probable cause Indicates that this chassis type is not compatible with the control processor (CP) blade.

Recommended action Use the CP blade on a compatible chassis.

Severity CRITICAL

SYSM-1007

Message `<timestamp>, [SYSM-1007], <sequence-number>,, WARNING, <system-name>, PERMITTING USE OF INCOMPATIBLE CHASSIS FOR CP IN SLOT <Slot number>. DATA ERRORS MAY RESULT.`

Probable cause Over-riding the incompatible control processor (CP)/chassis check. For engineering use only.

Recommended action Delete the /var/chassis_backplane_override file and reboot the CP.

Severity WARNING

83

TAPE Messages

This chapter contains information on the following TAPE message:

- TAPE-1001 780

TAPE-1001

Message

```
<timestamp>, [TAPE-1001], <sequence-number>, FFDC, INFO,
<system-name>, Key acquisition for <Pool or
Container><Begins or Complete>.
```

Probable Cause Indicates that the key acquisition for the pool or the container has begun or is complete.

Recommended Action No action is required.

Severity INFO

84

TRCE System Messages

This chapter contains information on the following TRCE messages:

- TRCE-1001 782
- TRCE-1002 782
- TRCE-1003 783
- TRCE-1004 783
- TRCE-1005 783
- TRCE-1006 784
- TRCE-1007 784
- TRCE-1008 784
- TRCE-1009 785
- TRCE-1010 785
- TRCE-1011 786
- TRCE-1012 786

TRCE-1001

Message

```
<timestamp>, [TRCE-1001], <sequence-number>,, WARNING,
<system-name>, Trace dump available< optional slot
indicating on which slot the dump occurs >! (reason:
<Text explanation of what triggered the dump. (PANIC
DUMP, WATCHDOG EXPIRED, MANUAL, TRIGGER)>)
```

Probable cause

Indicates that trace dump files have been generated on the switch or the indicated slot. The reason field indicates the cause for generating the dump as one of the following:

- PANICDUMP generated by panic dump
- WATCHDOG EXPIRED generated by hardware watchdog expiration
- MANUAL generated by the **tracedump -n** command

Recommended action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

TRCE-1002

Message

```
<timestamp>, [TRCE-1002], <sequence-number>,, INFO,
<system-name>, Trace dump< optional slot indicating on
which slot the dump occurs > automatically transferred to
FTP address ' <FTP target designated by user> '.
```

Probable cause

Indicates that a trace dump has occurred on the switch or the indicated slot and is successfully transferred from the switch automatically.

Recommended action

No action is required.

Severity

INFO

TRCE-1003

Message

```
<timestamp>, [TRCE-1003], <sequence-number>,, ERROR,
<system-name>, Trace dump< optional slot indicating on
which slot the dump occurs > was not transferred due to
FTP error.
```

Probable cause

Indicates that a trace dump has been created on the switch or the indicated slot but is not automatically transferred from the switch due to an FTP error, such as a wrong FTP address, FTP site down, or network down.

Recommended action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

TRCE-1004

Message

```
<timestamp>, [TRCE-1004], <sequence-number>,, WARNING,
<system-name>, Trace dump< optional slot indicating on
which slot the dump occurs > was not transferred because
trace auto-FTP disabled.
```

Probable cause

Indicates that trace dump files have been created on the switch or the indicated slot but are not automatically transferred from the switch because auto-FTP is disabled.

Recommended action

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

TRCE-1005

Message

```
<timestamp>, [TRCE-1005], <sequence-number>,, ERROR,
<system-name>, FTP Connectivity Test failed due to error.
```

Probable cause

Indicates that the connectivity test to the FTP host fails, because of an FTP error such as a wrong FTP address, an FTP site down, or the network being down.

Recommended action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

TRCE-1006

Message

```
<timestamp>, [TRCE-1006], <sequence-number>,, INFO,
<system-name>, FTP Connectivity Test succeeded to FTP
site ' <FTP target configured by users.> '.
```

Probable cause Indicates that a connectivity test to the FTP host has succeeded. This feature is enabled by the **supportFtp -t** command.

Recommended action No action is required.

Severity INFO

TRCE-1007

Message

```
<timestamp>, [TRCE-1007], <sequence-number>,, ERROR,
<system-name>, Notification of this CP has failed.
Parameters temporarily out of synch with other CP.
```

Probable cause Indicates that the active CP is unable to alert the standby CP of a change in trace status. This message is only applicable to enterprise-class platforms.

Recommended action This message is often transitory. Wait a few minutes and try the command again.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

TRCE-1008

Message

```
<timestamp>, [TRCE-1008], <sequence-number>, FFDC,
CRITICAL, <system-name>, Unable to load trace parameters.
```

Probable cause Indicates that the active CP is unable to read stored trace parameters.

Recommended action Reboot the CP (dual-CP system) or restart the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity CRITICAL

TRCE-1009

Message

```
<timestamp>, [TRCE-1009], <sequence-number>,, ERROR,
<system-name>, Unable to alert active CP that a dump has
occurred.
```

Probable cause Indicates that the standby CP is unable to communicate trace information to active CP. This message is only applicable to enterprise-class platforms.

Recommended action Run the **haShow** command to verify that the current CP is standby and the active CP is active.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

TRCE-1010

Message

```
<timestamp>, [TRCE-1010], <sequence-number>,, ERROR,
<system-name>, Traced fails to start
```

Probable cause Indicates that the trace daemon (traced), used for transferring trace files, failed to start. The trace capability within the switch is unaffected. The traced facility is normally restarted automatically by the system after a brief delay.

Recommended action If the message persists, reboot the CP (dual-CP system) or restart the switch.

Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity ERROR

TRCE-1011

Message

```
<timestamp>, [TRCE-1011], <sequence-number>,, INFO,
<system-name>, Trace dump manually transferred to target
' <optional string to indicate which slot the dump is
ftped out.> ': <result>.
```

Probable cause Indicates that a manual transfer of trace dump files has occurred.

Recommended action No action is required.

Severity INFO

TRCE-1012

Message

```
<timestamp>, [TRCE-1012], <sequence-number>,, WARNING,
<system-name>, The system was unable to retrieve trace
information from slot <Slot number of the blade the
attempt was made on>.
```

Probable cause Indicates that communication between the main system and the indicated slot is unavailable.

Recommended action Check that the AP blade is enabled and retry the command. If the AP blade is already enabled, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

85

TRCK System Messages

This chapter contains information on the following TRCK messages:

- TRCK-1001 788
- TRCK-1002 788
- TRCK-1003 788
- TRCK-1004 789
- TRCK-1005 789
- TRCK-1006 789

TRCK-1001

Message

```
<timestamp>, [TRCK-1001], <sequence-number>,, INFO,
<system-name>, Successful login by user <User>.
```

Probable cause Indicates that the track change feature recorded a successful login.

Recommended action No action is required.

Severity INFO

TRCK-1002

Message

```
<timestamp>, [TRCK-1002], <sequence-number>,, INFO,
<system-name>, Unsuccessful login by user <User>.
```

Probable cause Indicates that the track change feature recorded a failed login. This occurs if the user name or password is entered incorrectly.

Recommended action Normally, this message indicates a typing error by an authorized user. If this message occurs repeatedly, it might indicate an unauthorized user trying to gain access to a switch. When Secure mode is enabled on the fabric, the IP address of a failed login is reported to the error log.

Severity INFO

TRCK-1003

Message

```
<timestamp>, [TRCK-1003], <sequence-number>,, INFO,
<system-name>, Logout by user <User>.
```

Probable cause Indicates that the track change feature recorded a successful logout.

Recommended action No action is required.

Severity INFO

TRCK-1004

Message

```
<timestamp>, [TRCK-1004], <sequence-number>,, INFO,
<system-name>, Config file change from task:<task>
```

Probable cause

Indicates that the track change feature recorded a configuration change for the switch. The track change feature records any change to the configuration file in nonvolatile memory, including a **configDownload**. This message is not generated for a **configUpload**. All configuration changes occur through the PDM server, so the PDMIPC is the only task possible.

Recommended action

No action is required. Run the **configShow** command to view the configuration file.

Severity

INFO

TRCK-1005

Message

```
<timestamp>, [TRCK-1005], <sequence-number>,, INFO,
<system-name>, Track-changes on
```

Probable cause

Indicates that the track change feature has been enabled.

Recommended action

No action is required. Run the **trackChangesSet 0** command to disable the track change feature.

Severity

INFO

TRCK-1006

Message

```
<timestamp>, [TRCK-1006], <sequence-number>,, INFO,
<system-name>, Track-changes off
```

Probable cause

Indicates that the track change feature has been disabled.

Recommended action

No action is required. Run the **trackChangesSet 1** command to enable the track changes feature.

Severity

INFO

86

TS System Messages

This chapter contains information on the following TS messages:

- TS-1001 792
- TS-1002 792
- TS-1006 793
- TS-1007 793
- TS-1008 794

TS-1001

Message

```
<timestamp>, [TS-1001], <sequence-number>,, WARNING,
<system-name>, NTP Query failed: <error code>
```

Probable cause

Indicates that a network time protocol (NTP) query to the configured external clock server failed. Local clock time on the principal or primary fabric configuration server (FCS) switch is used for fabric synchronization.

This might be logged during temporary operational issues such as IP network connection issues to the external clock server. If it does not recur, it can be ignored.

Recommended action

Verify that the configured external clock server is available and functional. If that external clock server is not available, choose another.

Severity

WARNING

TS-1002

Message

```
<timestamp>, [TS-1002], <sequence-number>,, INFO,
<system-name>, < Type of clock server used > Clock Server
used instead of < Type of clock server configured >:
locl: 0x<code> remote: 0x<code>
```

Probable cause

Indicates that the fabric time synchronization distributed from the principal or primary fabric configuration server (FCS) switch was not sourced from the *Type of clock server configured*, instead, an alternate server was used, indicated by *Type of clock server used*. The type of clock server used or configured might be either one of the following:

- LOCL
  Local clock on the principal or primary FCS switch
- External
  External NTP server address configured

This might be logged during temporary operational issues such as IP network connection issues to the external clock server or if the fabric is configured for external time synchronization but the principal or primary FCS does not support the feature. If the message does not recur, it should be ignored.

Recommended action Run the **tsClockServer** command to verify that the principal or primary FCS switch has the clock server IP configured correctly. Verify that this clock server is accessible to the switch and functional. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

Severity INFO

TS-1006

Message `<timestamp>, [TS-1006], <sequence-number>,, INFO, <system-name>, <message>`

Probable cause Indicates that a time service event is occurring or has failed. The message might be one of the following:

- Init failed. Time Service exiting
  Probable cause: Initialization error, Time Server exits.
- Synchronizing time of day clock
  Probable cause: Usually logged during temporary operational issues when the clock goes out of synchronization: For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary fabric configuration server (FCS) switch. If the message does not recur, it should be ignored.
- Validating time update
  Probable cause: Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it should be ignored.

Recommended action No action is required.

Severity INFO

TS-1007

Message `<timestamp>, [TS-1007], <sequence-number>,, WARNING, <system-name>, <message>`

Probable cause Indicates that a switch is trying to set the tsclockserver, which is not the primary fabric configuration server (FCS) across the fabric. A consistent FCS policy must be implemented across the fabric.

Recommended action Verify that the FCS policy is consistent across the fabriclog_ts.xml.

Severity INFO

TS-1008

Message

```
<timestamp>, [TS-1008], <sequence-number>,, WARNING,
<system-name>, <New clock server used> Clock Server used
instead of <Old server configured>.
```

Probable cause Indicates that there is a change in the source of fabric time synchronization distributed from the principal or primary fabric configuration server (FCS) switch. Another clock server in the list of clock servers configured is being used. This happens when the network time protocol (NTP) query to the current active external clock server fails.

Recommended action No action is required.

Severity WARNING

87

UCST System Messages

This chapter contains information on the following UCST messages:

- UCST-1003 796
- UCST-1007 796
- UCST-1020 796
- UCST-1025 797
- UCST-1026 797
- UCST-1027 797

UCST-1003

Message

```
<timestamp>, [UCST-1003], <sequence-number>,, INFO,
<system-name>, Duplicate Path to Domain <domain ID>,
Output Port = <port number>, PDB pointer = 0x<value>
```

Probable cause Indicates that duplicate paths were reported to the specified domain from the specified output port. The path database (PDB) pointer is the address of the path database and provides debugging information.

Recommended action No action is required.

Severity INFO

UCST-1007

Message

```
<timestamp>, [UCST-1007], <sequence-number>, FFDC,
CRITICAL, <system-name>, Inconsistent route detected:
Port = <port number>, should be <port number>
```

Probable cause Indicates that the switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

Recommended action Run the **switchDisable** command and then the **switchEnable** command to reset the routing database. Run the **uRouteShow** command to display the new routing tables.

Severity CRITICAL

UCST-1020

Message

```
<timestamp>, [UCST-1020], <sequence-number>,, WARNING,
<system-name>, Static route (input-area: <port number>,
domain: <domain ID> output-area: <port number>) has been
ignored due to platform limitation.
```

Probable cause Indicates that the configured static route cannot be applied to the routing database due to a platform limitation.

Recommended action No action is required.

Severity WARNING

UCST-1025

Message `<timestamp>, [UCST-1025], <sequence-number>,, INFO, <system-name>, In-order delivery option has been enabled with Lossless-DLS option.`

Probable Cause Indicates the IOD option has been enabled for the switch. This option guarantees in-order delivery of frames during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1026

Message `<timestamp>, [UCST-1026], <sequence-number>,, INFO, <system-name>, LossLess-DLS option has been enabled.`

Probable Cause Indicates that the NoFrameDrop option is enabled. This will help minimize frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1027

Message `<timestamp>, [UCST-1027], <sequence-number>,, INFO, <system-name>, LossLess-DLS option has been disabled.`

Probable Cause Indicates that the NoFrameDrop option is disabled. This may cause higher frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

88

UPTH System Messages

This chapter contains information on the following UPTH message:

- UPTH-1001 800

UPTH-1001

Message

```
<timestamp>, [UPTH-1001], <sequence-number>,, WARNING,
<system-name>, No minimum cost path in candidate list
```

Probable cause

Indicates that the specified switch is unreachable because no minimum cost path (FSPF UPATH) exists in the candidate list (domain ID list).

Recommended action

No action is required. This will end the current SPF computation.

Severity

WARNING

89

WEBD System Messages

This chapter contains information on the following WEBD messages:

- WEBD-1001 802
- WEBD-1002 802
- WEBD-1004 802
- WEBD-1005 803
- WEBD-1006 803
- WEBD-1007 803
- WEBD-1008 804

WEBD-1001

Message `<timestamp>, [WEBD-1001], <sequence-number>,, WARNING, <system-name>, Missing or Invalid Certificate file -- HTTPS is configured to be enabled but could not be started.`

Probable cause Indicates that the SSL certificate file is either invalid or absent.

Recommended action Install a valid key file.

Severity WARNING

WEBD-1002

Message `<timestamp>, [WEBD-1002], <sequence-number>,, WARNING, <system-name>, Missing or Invalid Key file -- HTTPS is configured to be enabled but could not be started.`

Probable cause Indicates that the SSL key file is either invalid or absent.

Recommended action Install a valid key file.

Severity WARNING

WEBD-1004

Message `<timestamp>, [WEBD-1004], <sequence-number>,, INFO, <system-name>, HTTP server will be restarted due to configuration change`

Probable cause Indicates that the HTTP server configuration has changed.

Recommended action No action is required.

Severity INFO

WEBD-1005

Message `<timestamp>, [WEBD-1005], <sequence-number>,, WARNING, <system-name>, HTTP server will be restarted for logfile truncation`

Probable cause Indicates that the size of HTTP logfile exceeded the maximum limit.

Recommended action No action is required.

Severity WARNING

WEBD-1006

Message `<timestamp>, [WEBD-1006], <sequence-number>,, INFO, <system-name>, HTTP server restarted due to logfile truncation`

Probable cause Indicates that the size of HTTP logfile exceeded the maximum limit.

Recommended action No action is required.

Severity INFO

WEBD-1007

Message `<timestamp>, [WEBD-1007], <sequence-number>, FFDC, INFO, <system-name>, HTTP server will be restarted due to change of IP Address`

Probable cause Indicates that the IP address of the switch changed and the HTTP server is restarted.

Recommended action No action is required.

Severity INFO

WEBD-1008

Message

```
<timestamp>, [WEBD-1008], <sequence-number>, FFDC,
WARNING, <system-name>, HTTP server cannot be started
```

Probable cause

Indicates a rare error condition, where the built-in recovery process has failed to restore http services. The problem often results from invalid configuration of ssl certs., but there can be more than one reason for such failure.

Recommended action

Reboot the switch to restart HTTP/HTTPS.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

90

ZOLB System Messages

This chapter contains information on the following ZOLB message:

- ZOLB-1001 806

ZOLB-1001

Message

```
<timestamp>, [ZOLB-1001], <sequence-number>,, ERROR,
<system-name>, ZONELIB <error message>
```

Probable cause

Indicates that there was an internal timeout on the inter process communication (IPC) between the name server (NS) and the zoning modules. This usually indicates that the system was busy.

Recommended action

This message generates core dump files of the related modules (zoned, nsd, rcsd).

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command to save these core files and contact the EMC Customer Support Center.

Severity

ERROR

91

ZONE System Messages

This chapter contains information on the following ZONE messages:

- ZONE-1002 809
- ZONE-1003 809
- ZONE-1004 809
- ZONE-1005 810
- ZONE-1006 811
- ZONE-1007 811
- ZONE-1008 812
- ZONE-1010 812
- ZONE-1012 812
- ZONE-1013 813
- ZONE-1014 813
- ZONE-1015 813
- ZONE-1017 814
- ZONE-1018 814
- ZONE-1019 815
- ZONE-1022 815
- ZONE-1023 816
- ZONE-1024 816
- ZONE-1026 816
- ZONE-1027 817
- ZONE-1028 817
- ZONE-1029 818
- ZONE-1030 818
- ZONE-1031 819
- ZONE-1032 819
- ZONE-1033 819
- ZONE-1034 820

- ZONE-1035 820
- ZONE-1036 820
- ZONE-1037 821
- ZONE-1038 821
- ZONE-1039 821
- ZONE-1040 822
- ZONE-1041 822
- ZONE-1042 822
- ZONE-1043 823
- ZONE-1044 823
- ZONE-1045 823
- ZONE-1046 824
- ZONE-1047 824
- ZONE-1048 824
- ZONE-1049 825
- ZONE-1050 825
- ZONE-1051 825
- ZONE-1052 826
- ZONE-1053 826

ZONE-1002

Message

```
<timestamp>, [ZONE-1002], <sequence-number>,, WARNING,
<system-name>, WWN zoneTypeCheck or zoneGroupCheck
warning(<warning string>) at port(<port number>)
```

Probable cause

Indicates that a zone filter or zone group check failure occurred. The frame filter logic reported a failure when creating or adding zone groups during port login (PLOGI) trap processing. This messages usually indicates problems when adding content-addressable memory (CAM) entries before the filter setup.

Recommended action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

WARNING

ZONE-1003

Message

```
<timestamp>, [ZONE-1003], <sequence-number>,, WARNING,
<system-name>, zone(<current zone>) contains (<domain
id>, <port number>) which does not exist.
```

Probable cause

Indicates that the port zone member that is targeted for the local switch contains a non-existent port. The effective zoning configuration (displayed in the error message) contains a port number that is out of range.

Recommended action

Edit the zone database and change the port number to a viable value in the effective configuration.

Severity

WARNING

ZONE-1004

Message

```
<timestamp>, [ZONE-1004], <sequence-number>,, INFO,
<system-name>, port <port number> enforcement changed to
Session Based HARD Zoning.
```

Probable cause

Indicates that the zoning enforcement changed to session-based hard zoning. When a device is zoned using both world-wide name

(WWN) in one zone and <*domain, portarea*> in another, this will cause that port to go session based hard zoning.

In session-based zoning, the zone enforcement is checked by the software. In hardware-enforced zoning, zone or alias members are defined using <domain, portarea> exclusively or using WWNs exclusively: that is, using one method or the other to define all objects in the zoning database. If the devices on the port are defined by a mixture of port IDs and WWNs, the zone enforcement is session based. If the S_ID list of the hardware-enforced zoning overflows (over the S_ID limit), the hardware zone enforcement changes to session-based zoning.

Recommended action No action is required.

Severity INFO

ZONE-1005

Message `<timestamp>, [ZONE-1005], <sequence-number>,, INFO, <system-name>, HARD & SOFT zones(<zone name>, <zone name>) definitions overlap.`

Probable cause Indicates that a port is zoned with mixed devices (world-wide name (WWN) and <*domain, portarea*>). During zoning database cross checking, it is detected that either:

- A port zone member is also listed as a member of a Mixed zone,
- A world-wide name (WWN) zone member is also specified as a member of a Mixed zone.

You should use hard zone enforcement whenever possible. Hard zones are more secure than “session-based hard zones”. Both types of zones will trap a port login (PLOGI), but hard zones will filter out the I/O frames which”session-based” hard zones do not.

Recommended action If hard zone enforcement is preferred, edit the zoning database to have the port zoned with devices defined as either WWN or defined as <*domain, portarea*> but do not mix the methods used to define these zone members.

Severity INFO

ZONE-1006

Message

```
<timestamp>, [ZONE-1006], <sequence-number>,, WARNING,
<system-name>, WARNING - WWN(<WWN number>) in HARD PORT
zone <zone_name>.
```

Probable cause

Indicates that one or more devices are zoned as world-wide name (WWN) devices and also zoned as <*domain, portarea*> devices. The device(s) are used to specify zone members over separate zones.

Recommended action

If hardware zoning enforcement is preferred, edit the zoning database to have the device zoned using only one specification type, either WWN or <*domain, portarea*>.

Severity

WARNING

ZONE-1007

Message

```
<timestamp>, [ZONE-1007], <sequence-number>,, INFO,
<system-name>, Ioctl(<function>) in (<error message>) at
port (<port number>) returns code (<error string>) and
reason string (<reason string>).
```

Probable cause

Indicates that frame filter logic reported a failure during one of the IOCTL calls. The IOCTL call from which the failure is reported is listed as part of the error message. This is usually a programming error when adding content-addressable memory (CAM) entries before the filter setup.

Recommended action

There are two ways to avoid this problem.

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

Severity

INFO

ZONE-1008

Message `<timestamp>, [ZONE-1008], <sequence-number>,, WARNING, <system-name>, WARNING - port <port number> Out of CAM entries.`

Probable cause Indicates that the total number of entries of S_ID CAM is above the limit while creating or adding a zone group. The maximum number of content-addressable memory (CAM) entries allowed depends on the application-specific integrated circuit (ASIC).

Recommended action If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

Severity WARNING

ZONE-1010

Message `<timestamp>, [ZONE-1010], <sequence-number>,, WARNING, <system-name>, WARNING - Duplicate entries in zone(<zone name>) specification.`

Probable cause Indicates that there are duplicate entries in a zone object. A zone object member is specified twice in a given zone object. This message occurs only when enabling a zone configuration.

Recommended action Check the members of the zone and delete the duplicate member.

Severity WARNING

ZONE-1012

Message `<timestamp>, [ZONE-1012], <sequence-number>,, WARNING, <system-name>, WARNING - All ports are offline.`

Probable cause Indicates that all the ports in a zone are offline.

Recommended action Check the device connection.

Severity WARNING

ZONE-1013

Message `<timestamp>, [ZONE-1013], <sequence-number>,, WARNING, <system-name>, Quick Loop not supported.`

Probable cause Indicates that the QuickLoop feature is not supported in the current code release. If the QuickLoop zoning configuration is enabled on the switch, it will not be supported.

Recommended action Edit the zone database to remove the QuickLoop zoning definition in the effective configuration.

Severity WARNING

ZONE-1014

Message `<timestamp>, [ZONE-1014], <sequence-number>,, ERROR, <system-name>, Missing required license - <license name>.`

Probable cause Indicates that the required zoning license is missing.

Recommended action Install the zoning license using the **licenseAdd** command. Refer to your EMC account representative to obtain a Zoning license if you do not have one.

Severity ERROR

ZONE-1015

Message `<timestamp>, [ZONE-1015], <sequence-number>,, WARNING, <system-name>, Not owner of the current transaction <transaction ID>.`

Probable cause Indicates that a zoning change operation is not allowed because the zoning transaction is opened by another task. Indicates concurrent modification of the zone database by multiple administers.

Recommended action Wait until the previous transaction is completed. Verify that only one administrator is working with the zone database at a time.

Severity WARNING

ZONE-1017

Message

```
<timestamp>, [ZONE-1017], <sequence-number>,, ERROR,
<system-name>, FA Zone(<zone name>) contains incorrect
number of Initiator and Target devices.
```

Probable cause

Indicates that the fabric assist (FA) zoning configuration has more than one initiator. The probable cause is incorrect entries in the FA zoning configuration.

Recommended action

Edit the zone database to ensure that only one initiator is set for each FA zone configuration.

Severity

ERROR

ZONE-1018

Message

```
<timestamp>, [ZONE-1018], <sequence-number>,, ERROR,
<system-name>, Incorrect zoning enforcement type(<zone
type>) at port(<port number>).
```

Probable cause

Indicates that an incorrect zoning enforcement type was reported on the specified port. This is a software error. A QuickLoop zone type (value = 4) or an uninitialized type (value = 0) are invalid. The valid zone type values are:

- hard port zone (value = 1)
- hard wwn zone (value = 2)
- session based hard zoning (value = 3)
- FA zone (value = 5)

QuickLoop zones are not supported in Fabric OS v4.x and above.

Recommended action

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

ZONE-1019

Message

```
<timestamp>, [ZONE-1019], <sequence-number>,, ERROR,
<system-name>, Transaction Commit failed. Reason code
<reason code> (<Application reason>) - \"<reason
string>\"
```

Probable cause

Indicates that the reliable commit service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

Recommended action

Often this message indicates a transitory problem. Wait a few minutes and retry the command.

Make sure that your changes to the zone database are not overwriting the work of another admin.

Run the **cfgTransShow** command to find out if there is any outstanding transaction running on the local switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

ERROR

ZONE-1022

Message

```
<timestamp>, [ZONE-1022], <sequence-number>,, INFO,
<system-name>, The effective configuration has changed to
<Effective configuration name>. <AD Id>
```

Probable cause

Indicates that the effective zone configuration has changed to the name displayed.

Recommended action

Verify that this zone configuration change was done on purpose. If the new effective zone configuration is correct, no action is necessary.

Severity

INFO

ZONE-1023

Message `<timestamp>, [ZONE-1023], <sequence-number>,, INFO, <system-name>, Switch connected to port (<port number>) is busy. Retry zone merge.`

Probable cause Indicates that the switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

Recommended action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

ZONE-1024

Message `<timestamp>, [ZONE-1024], <sequence-number>,, INFO, <system-name>, <Information message>.`

Probable cause Indicates that the **cfgSave** command ran successfully. The <*Information message*> is "cfgSave completes successfully."

Recommended action No action is required.

Severity INFO

ZONE-1026

Message `<timestamp>, [ZONE-1026], <sequence-number>,, INFO, <system-name>, port <port number> Out of CAM entries.`

Probable cause Indicates that the total number of S_ID entries while creating or adding a zone group exceeds the limit.

Recommended action If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

Severity INFO

ZONE-1027

Message

```
<timestamp>, [ZONE-1027], <sequence-number>,, INFO,
<system-name>, Zoning transaction aborted <error reason>.
<AD Id>.
```

Probable cause

Indicates that the zoning transaction was aborted due to a variety of potential errors. The *error reason* variable can be one of the following:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new config is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell has exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

Recommended action

Many of the causes of this error message are transitory: for example because two admins are working with the zoning database concurrently. If you receive this error, wait a few minutes and try again. Verify that no one else is currently modifying the zone database.

Severity

INFO

ZONE-1028

Message

```
<timestamp>, [ZONE-1028], <sequence-number>,, WARNING,
<system-name>, Commit zone DB larger than supported -
<zone db size> greater than <max zone db size>.
```

Probable cause

Indicates that the zone database size is greater than the limit allowed by the fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended action Edit the zone database to keep it within the allowable limit for the specific switches in your fabric. Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for information on the zone database sizes supported for each switch.

Severity WARNING

ZONE-1029

Message `<timestamp>, [ZONE-1029], <sequence-number>,, WARNING, <system-name>, Restoring zone cfg from flash failed - bad config saved to <config file name> [<return code>].`

Probable cause Indicates that the zone configuration restored from the flash was faulty.

Recommended action This error will save the faulty zone configuration in the zoned core file directory.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity WARNING

ZONE-1030

Message `<timestamp>, [ZONE-1030], <sequence-number>,, WARNING, <system-name>, Converting the zone db for PID format change failed.`

Probable cause Indicates that the current zone database could not be converted to reflect the PID format change. Most likely this is caused by the size of the zone database.

Recommended action Change the PID format back to its original format. Reduce the size of the zone database. Then you can change the PID format to the requested format.

Severity WARNING

ZONE-1031

Message `<timestamp>, [ZONE-1031], <sequence-number>,, ERROR, <system-name>, Switch is in interop mode. (switch, port) members not supported.`

Probable cause The switch is set to interop mode using the **interopMode** command. Interop mode does not allow <*domain, portarea*> members in the active zone database.

Recommended action Remove all <*domain, portarea*> members from the zone database, or convert them to world-wide name (WWN) zoning.

Severity ERROR

ZONE-1032

Message `<timestamp>, [ZONE-1032], <sequence-number>,, ERROR, <system-name>, Domain <domain number> Max Zone DB size <max zone db size>.`

Probable cause Indicates that the specified domain does not have enough memory for the zone database being committed.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1033

Message `<timestamp>, [ZONE-1033], <sequence-number>,, ERROR, <system-name>, Domain <domain number> Lowest Max Zone DB size.`

Probable cause Indicates that the specified domain has the lowest memory available for the zone database in the fabric. The zone database must be smaller than the memory available on this domain.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1034

Message `<timestamp>, [ZONE-1034], <sequence-number>,, WARNING, <system-name>,A new zone database file was successfully created for the switch.`

Probable cause Indicates that a new zone database file was successfully created for the switch.

Recommended action No action is required.

Severity WARNING

ZONE-1035

Message `<timestamp>, [ZONE-1035], <sequence-number>,, ERROR, <system-name>, Unable to rename <Old config file name> to <New config file name>: error message <System Error Message>`

Probable cause Indicates that the Fabric OS cannot rename the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1036

Message `<timestamp>, [ZONE-1036], <sequence-number>,, ERROR, <system-name>, Unable to create <config file name>: error message <System Error Message>`

Probable cause Indicates that the Fabric OS cannot create the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1037

Message `<timestamp>, [ZONE-1037], <sequence-number>,, ERROR, <system-name>, Unable to examine <config file name>: error message <System Error Message>.`

Probable cause Indicates that the Fabric OS cannot examine the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1038

Message `<timestamp>, [ZONE-1038], <sequence-number>,, ERROR, <system-name>, Unable to allocate memory for <config file name>: error message <System Error Message>.`

Probable cause Indicates that the Fabric OS cannot allocate enough memory for the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1039

Message `<timestamp>, [ZONE-1039], <sequence-number>,, ERROR, <system-name>, Unable to read contents of <config file name>: error message <System Error Message>`

Probable cause Indicates that the Fabric OS cannot read the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1040

Message

```
<timestamp>, [ZONE-1040], <sequence-number>,, INFO,
<system-name>, Merged zone database exceeds limit.
```

Probable cause Indicates that the Fabric OS cannot read the merged zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended action Reduce the size of the zone database and retry the operation.

Severity INFO

ZONE-1041

Message

```
<timestamp>, [ZONE-1041], <sequence-number>,, WARNING,
<system-name>, Unstable link detected during merge at
port (<Port number>).
```

Probable cause Indicates a possible unstable link or faulty cable.

Recommended action Check the SFP and cable at the specified port and verify that they are not faulty. Replace the SFP and cable as necessary.

Severity WARNING

ZONE-1042

Message

```
<timestamp>, [ZONE-1042], <sequence-number>,, INFO,
<system-name>, The effective configuration has been
disabled. <AD Id>.
```

Probable cause Indicates that the effective zone configuration has been disabled.

Recommended action Verify that this zone configuration change was done on purpose. If no effective zone configuration is needed, no action is necessary.

Severity INFO

ZONE-1043

Message `<timestamp>, [ZONE-1043], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is set to No Access.`

Probable cause Indicates that the Default Zone access mode is set to No Access.

Recommended action Verify that this Default Zone access mode change was done intentionally.

Severity INFO

ZONE-1044

Message `<timestamp>, [ZONE-1044], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is set to All Access.`

Probable cause Indicates that the Default Zone access mode is set to All Access.

Recommended action Verify that this Default Zone access mode change was done intentionally.

Severity INFO

ZONE-1045

Message `<timestamp>, [ZONE-1045], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is already set to No Access.`

Probable cause Indicates that the Default Zone access mode is already set to No Access.

Recommended action No action is required.

Severity INFO

ZONE-1046

Message `<timestamp>, [ZONE-1046], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is already set to All Access.`

Probable cause Indicates that the Default Zone access mode is already set to All Access.

Recommended action No action is required.

Severity INFO

ZONE-1047

Message `<timestamp>, [ZONE-1047], <sequence-number>,, INFO, <system-name>, Switch domain (<domainr>) does not support defined database.`

Probable Cause Indicates that remote B-Series switch is running a downlevel version of Fabric OS that does not support the defined database.

Recommended Action Run the **firmwareDownload** command to upgrade all swtiches to same release level version.

Severity INFO

ZONE-1048

Message `<timestamp>, [ZONE-1048], <sequence-number>,, WARNING, <system-name>, SZONE ACA is rejected on the standby.`

Probable Cause Indicates that the standby zoning component has not received a **syncdump** command from the primary side.

Recommended Action Run the **haSyncStart** command to synchronize the standby CP.

Severity WARNING

ZONE-1049

Message `<timestamp>, [ZONE-1049], <sequence-number>,, ERROR, <system-name>, ZONE AD-DefZone conflict detected while system initialization.`

Probable Cause Indicates that there is an AD-DefZone conflict.

Recommended Action Check and resolve the default zone mismatch issue.

Severity ERROR

ZONE-1050

Message `<timestamp>, [ZONE-1050], <sequence-number>,, INFO, <system-name>, The Interop Safe Zoning mode is set to Enabled.`

Probable Cause Indicates that the Interop Safe Zoning mode is enabled.

Recommended Action Verify if the Safe Zoning mode change was done on purpose.

Severity INFO

ZONE-1051

Message `<timestamp>, [ZONE-1051], <sequence-number>,, INFO, <system-name>, The Interop Safe Zoning mode is set to Disabled.`

Probable Cause Indicates that the Interop Safe Zoning mode is disabled.

Recommended Action Verify if the Safe Zoning mode change was done on purpose.

Severity INFO

ZONE-1052

Message `<timestamp>, [ZONE-1052], <sequence-number>,, INFO, <system-name>, The Interop Default Zone state is set to enabled.`

Probable Cause Indicates the Interop Default Zone attribute state is enabled.

Recommended Action Verify if the Interop Default Zone attribute state change was done on purpose.

Severity INFO

ZONE-1053

Message `<timestamp>, [ZONE-1053], <sequence-number>,, INFO, <system-name>, The Default Zone state is set to Disabled.`

Probable Cause Indicates the Interop Default Zone attribute state is disabled.

Recommended Action Verify if the Interop Default Zone attribute state change was done on purpose.

Severity INFO

PART 2

Audit Log Messages

This section provides the Audit Log messages.

For a list of these messages, refer to the Table of Contents on page 3

92

AUDIT AG System Messages

This chapter contains information on the following AUDIT AG message:

- AG-1029 830

AG-1029

Message AUDIT, <timestamp>, [AG-1029], INFO, CFG, <event-initiator-details>, <event-location>, , F_Port to N_Port mapping has been updated for N_Port <n_port>.

Probable Cause Indicates that the F_Ports mapped to an N_Port have changed and the config file has been updated.

RecommendedAction No action is required.

Severity INFO

93

AUDIT AUTH System Messages

This chapter contains information on the following AUDIT AUTH messages:

- AUTH-3001 832
- AUTH-3002 832
- AUTH-3003 832
- AUTH-3004 833
- AUTH-3005 833
- AUTH-3006 834
- AUTH-3007 834
- AUTH-3008 835

AUTH-3001

Message

```
AUDIT, <timestamp>, [AUTH-3001], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Data type> type has
been changed from [<Old value>] to [<New value>].
```

Probable Cause Indicates that an authentication configuration value was set to a specified value. The *data type* is "authentication type", "DH group type", "Hash type", or "policy type".

Recommended Action No action is required.

Severity INFO

AUTH-3002

Message

```
AUDIT, <timestamp>, [AUTH-3002], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Event Related
Info>.
```

Probable Cause Indicates that the secret database operation has been updated using the **secAuthSecret** command.

Recommended Action No action is required.

Severity INFO

AUTH-3003

Message

```
AUDIT, <timestamp>, [AUTH-3003], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Operation type> the
PKI objects.
```

Probable Cause Indicates that the public key infrastructure (PKI) objects were created using the **pkiCreate** command or that the PKI objects were removed using the **pkiRemove** command. The *Operation Type* can be either "Created" or "Removed".

Recommended Action No action is required.

Severity INFO

AUTH-3004

Message

```
AUDIT, <timestamp>, [AUTH-3004], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Neighboring switch
has a conflicting authentication policy; Port <Port
Number> disabled.
```

Probable Cause The specified E_Port was disabled because the neighboring switch rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action Correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the specified port executing **portEnable**.

Severity INFO

AUTH-3005

Message

```
AUDIT, <timestamp>, [AUTH-3005], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Rejecting
authentication request on port <Port Number> because
switch policy is turned off.
```

Probable Cause Indicates that the local switch has rejected the authentication request, because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the light will go off due to conflicting configuration settings. Otherwise the E_Port will form without authentication.

Recommended Action If the light on the specified port is off, correct the switch policy configuration on either of the switches using **the authUtil** command, and then enable the port on the neighboring switch using the **portEnable** command. If the E_Port formed no action is required.

Severity INFO

AUTH-3006

Message

```
AUDIT, <timestamp>, [AUTH-3006], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Authentication failed
on port <port number> due to mismatch of DH-CHAP shared
secrets.
```

Probable Cause

Indicates that an authentication operation using a Diffie Hellman - challenge-handshake authentication protocol (DH-CHAP) failed on the specified port due to mismatched response values between two entities.

The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using **secAuthSecret** and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity

INFO

AUTH-3007

Message

```
AUDIT, <timestamp>, [AUTH-3007], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Port <port number>
disabled due to receiving an authentication reject with
code '<Reason String>' and explanation '<Explanation
String>'.
```

Probable Cause

Indicates that the specified port was disabled due to receiving an authentication reject response from the connected switch/device.

The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using **secAuthSecret** and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

AUTH-3008

Message

```
AUDIT, <timestamp>, [AUTH-3008], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Port <port number>
has been disabled due to authentication failure with code
'<Reason String>' and explanation '<Explanation String>'.
```

Probable Cause Indicates that the specified port has been disabled, because the connecting switch/device failed to authenticate.

The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action Check the connection port for a possible security attack.

Check the shared secrets using **secAuthSecret** and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact the EMC Customer Support Center.

Severity INFO

94

AUDIT CONF System Messages

This chapter contains information on the following AUDIT CONF messages:

- CONF-1000 854
- CONF-1020 854
- CONF-1022 854

CONF-1000

Message

```
AUDIT, <timestamp>, [CONF-1000], INFO, CFG,
<event-initiator-details>, <event-location>, ,
configDownload completed successfully. <Info about the
parameters and AD>.
```

Probable cause

The **configDownload** process was initiated and completed successfully. The message string describes the class of configuration parameters that were downloaded. If admin domain (AD) is enabled, the AD number is specified in the description.

Recommended action

No action is required.

Severity

INFO

CONF-1020

Message

```
AUDIT, <timestamp>, [CONF-1020], INFO, CFG,
<event-initiator-details>, <event-location>, ,
configDownload not permitted <AD Number if AD is
configured on the system>.
```

Probable cause

There are several possible causes.

Recommended action

Check the error log to determine the cause. Correct the error and retry the **configDownload** operation.

Severity

INFO

CONF-1022

Message

```
AUDIT, <timestamp>, [CONF-1022], WARNING, CFG,
<event-initiator-details>, <event-location>, ,
Downloading configuration without disabling the switch
was unsuccessful.
```

Probable cause

The system attempted to download a configuration without disabling the switch was unsuccessful because there are one or more parameters that require the switch to be disabled.

Recommended action Disable the switch using the **switchDisable** command and download the configuration.

Severity WARNING

95

AUDIT FCIP System Messages

This chapter contains information on the following AUDIT AUTH messages:

- FCIP-1002 842
- FCIP-1003 842

FCIP-1002

Message AUDIT, <timestamp>, [FCIP-1002], INFO, CFG, <event-initiator-details>, `<event-location>, , An IPsec/IKE policy was added.`

Probable Cause Indicates that an IPsec/IKE policy was added and the config file was updated.

Recommended Action No action is required.

Severity INFO

FCIP-1003

Message AUDIT, <timestamp>, [FCIP-1003], INFO, CFG, <event-initiator-details>, `<event-location>, , An IPsec/IKE policy was deleted.`

Probable Cause Indicates that an IPsec/IKE policy was deleted and the config file was updated.

Recommended Action No action is required.

Severity INFO

96

AUDIT FICU System Messages

This chapter contains information on the following AUDIT FICU messages:

- FICU-1011 844
- FICU-1012 844

FICU-1011

Message

```
AUDIT, <timestamp>, [FICU-1011], INFO, CFG,
<event-initiator-details>, <event-location>, , FMS mode
has been enabled.
```

Probable Cause Indicates the FICON Management server mode has been enabled.

Recommended Action No action is required.

Severity INFO

FICU-1012

Message

```
AUDIT, <timestamp>, [FICU-1012], INFO, CFG,
<event-initiator-details>, <event-location>, , FMS mode
has been disabled.
```

Probable Cause Indicates the FICON Management server mode has been disabled.

Recommended Action No action is required.

Severity INFO

97

AUDIT FW System Messages

This chapter contains information on the following AUDIT FW message:

- FW-3001 846

FW-3001

Message

```
AUDIT, <timestamp>, [FW-3001], INFO,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info:<Event Related info>
```

Probable cause Indicates that Port Fencing was enabled/disabled successfully.

Recommended action No action is required.

Severity INFO

98

AUDIT HTTP System Messages

This chapter contains information on the following AUDIT HTTP messages:

- HTTP-1002 864
- HTTP-1003 864

HTTP-1002

Message

```
AUDIT, <timestamp>, [HTTP-1002], INFO, ZONE,
<event-initiator-details>, <event-location>, , Zoning
transaction initiated by User: <User Name>, Role: <User
Role> completed successfully.
```

Probable cause Indicates that the zoning database has been changed.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

HTTP-1003

Message

```
AUDIT, <timestamp>, [HTTP-1003], INFO, ZONE,
<event-initiator-details>, <event-location>, , Zoning
transaction initiated by User: <User Name>, Role: <User
Role> could not be completed successfully - <Reason
Message>.
```

Probable cause Indicates an error occurred while completing the zoning transaction.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

99

AUDIT IPAD System Messages

This chapter contains information on the following AUDIT AUTH messages:

- IPAD-1002..... 866

IPAD-1002

Message

```
AUDIT, <timestamp>, [IPAD-1002], INFO, CFG,
<event-initiator-details>, <event-location>, , Switchname
has been successfully changed to <Switch name>.
```

Probable Cause Indicates that a change with the switch name has occured.

Recommended Action No action is required.

Severity INFO

100

AUDIT PORT System Messages

This chapter contains information on the following AUDIT FCIP messages:

- PORT-1006 852
- PORT-1007 852
- PORT-1008 852
- PORT-1009 853

PORT-1006

Message `AUDIT, <timestamp>, [PORT-1006], INFO, CFG, <event-initiator-details>, <event-location>, , Configuration changed for port (ID: <port number>) in No_Module or No_Light state.`

Probable Cause Indicates the configuration changes were made to an offline port in No_Module or No_Light state.

Recommended Action No action is required.

Severity INFO

PORT-1007

Message `AUDIT, <timestamp>, [PORT-1007], INFO, CFG, <event-initiator-details>, <event-location>, , Port (ID: <port number>) has been renamed to <port name>.`

Probable Cause Indicates a port has been reconfigured with a different name.

Recommended Action No action is required.

Severity INFO

PORT-1008

Message `AUDIT, <timestamp>, [PORT-1008], INFO, CFG, <event-initiator-details>, <event-location>, , GigE Port (ID: <port number>) has been enabled.`

Probable Cause Indicates a GigE port has been enabled.

Recommended Action No action is required.

Severity INFO

PORT-1009

Message

```
AUDIT, <timestamp>, [PORT-1009], INFO, CFG,
<event-initiator-details>, <event-location>, , GigE Port
(ID: <port number>) has been disabled.
```

Probable Cause

Indicates a GigE port has been disabled.

Recommended Action

No action is required.

Severity

INFO

101

AUDIT SEC System Messages

This chapter contains information on the following AUDIT SEC messages:

- SEC-3001 857
- SEC-3002 857
- SEC-3003 858
- SEC-3004 858
- SEC-3005 858
- SEC-3006 859
- SEC-3007 859
- SEC-3008 860
- SEC-3009 860
- SEC-3010 861
- SEC-3011 861
- SEC-3012 861
- SEC-3013 862
- SEC-3014 862
- SEC-3015 863
- SEC-3016 863
- SEC-3017 863
- SEC-3018 864
- SEC-3019 864
- SEC-3020 865
- SEC-3021 865
- SEC-3022 865
- SEC-3023 866
- SEC-3024 866
- SEC-3025 866
- SEC-3026 867

- SEC-3027 867
- SEC-3028 867
- SEC-3029 868
- SEC-3030 868
- SEC-3031 869
- SEC-3032 869
- SEC-3033 869
- SEC-3034 870
- SEC-3035 870
- SEC-3036 870
- SEC-3037 871
- SEC-3038 871
- SEC-3039 872
- SEC-3040 872
- SEC-3041 872
- SEC-3044 873
- SEC-3045 873
- SEC-3046 873
- SEC-3047 874
- SEC-3048 874
- SEC-3049 874
- SEC-3050 875
- SEC-3051 875

SEC-3001

Message

```
AUDIT, <timestamp>, [SEC-3001], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Security mode <State
change: Enabled or Disabled> on the fabric.
```

Probable cause

Indicates that the security mode of the fabric was either enabled or disabled.

Recommended action

Verify that the security mode change was planned. If the security mode change was planned, no action is required. If the security mode change was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3002

Message

```
AUDIT, <timestamp>, [SEC-3002], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Event Related
Info>.
```

Probable cause

Indicates that the specified security event has occurred. The *Event Name* can be one of the following:

- There has been an fabric configurations server (FCS) failover.
- A security policy has been activated.
- A security policy has been saved.
- A security policy has been aborted.
- A non-FCS password has changed.

Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3003

Message

```
AUDIT, <timestamp>, [SEC-3003], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Created <Policy
Name> policy, with member(s) <Member List> .
```

Probable cause

Indicates that a new security policy was created with entries.
Note: If you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the event info field.

Recommended action

Verify that the new policy creation was planned. If the new policy creation was planned, no action is required. If the new policy creation was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3004

Message

```
AUDIT, <timestamp>, [SEC-3004], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Created <Policy
name> policy.
```

Probable cause

Indicates that a new security policy was created.
Note: If you use a wildcard (for example, an asterisk) in creating a member for a policy, the audit message displays the wildcard in the event info field.

Recommended action

Verify that the new policy creation was planned. If the new policy creation was planned, no action is required. If the new policy creation was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3005

Message

```
AUDIT, <timestamp>, [SEC-3005], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Added member(s)
<Members added> to policy <Policy name>.
```

Probable cause Indicates that new member(s) have been added to the specified security policy.

Note: If you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event info field.

Recommended action Verify that the addition of members to the policy was planned. If the addition of members was planned, no action is required. If the addition of members was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3006

Message

```
AUDIT, <timestamp>, [SEC-3006], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Removed member(s)
<Members removed> from policy <Policy name>.
```

Probable cause Indicates that a user has removed the specific members from the specified security policy.

Note: If you use a wildcard (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the event info field.

Recommended action Verify that the removal of members to the policy was planned. If the removal of members was planned, no action is required. If the removal of members was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3007

Message

```
AUDIT, <timestamp>, [SEC-3007], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Deleted policy
<Deleted policy name>.
```

Probable cause Indicates that the specified security policy was deleted.

Recommended action Verify that the policy deletion was planned. If the policy deletion was planned, no action is required. If the policy deletion was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3008

Message

```
AUDIT, <timestamp>, [SEC-3008], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: FCS member moved
from position <Old FCS position> to <New FCS position>.
```

Probable cause Indicates that the fabric configurations server (FCS) list has been modified. One of the members of the list has been moved to a new position in the list, as identified in the message.

Recommended action Verify that the modification was planned. If the modification was planned, no action is required. If the modification was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3009

Message

```
AUDIT, <timestamp>, [SEC-3009], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Security Transaction
aborted.
```

Probable cause Indicates that the pending security transaction was aborted.

Recommended action Verify that the security transaction was intentionally aborted. If the security transaction was intentionally aborted, no action is required. If the security transaction was not intentionally aborted, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3010

Message

```
AUDIT, <timestamp>, [SEC-3010], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Reset [<Name of
security stat(s) reset>] security stat(s).
```

Probable cause Indicates that a user has reset all the security statistics.

Recommended action Verify that the security statistics were intentionally reset. If the security statistics were intentionally reset, no action is required. If the security statistics were not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3011

Message

```
AUDIT, <timestamp>, [SEC-3011], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Reset [<Stat name>]
statistics on domain(s) [<Domain IDs>].
```

Probable cause Indicates that a user has reset a security statistic on the specified domains.

Recommended action Verify that the security statistic was intentionally reset. If the security statistic were intentionally reset, no action is required. If the security statistic was not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3012

Message

```
AUDIT, <timestamp>, [SEC-3012], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Temp Passwd
<Password Set or Reset> on domain [<Domain ID>] for
account [<Account name>].
```

Probable cause Indicates that a user has reset the password for the specified user accounts.

Recommended action Verify that the password was intentionally reset. If the password was intentionally reset, no action is required. If the password was not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3013

Message

```
AUDIT, <timestamp>, [SEC-3013], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Security Version
stamp is reset.
```

Probable cause Indicates that a user has reset the security version stamp.

Recommended action Verify that the security version stamp was intentionally reset. If the security event was planned, no action is required. If the security version stamp was not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3014

Message

```
AUDIT, <timestamp>, [SEC-3014], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Event option>
RADIUS server <Server Name> for AAA services.
```

Probable cause Indicates that a user has changed the remote authentication dial-in user service (RADIUS) configuration.

Recommended action Verify that the RADIUS configuration was changed intentionally. If the RADIUS configuration was intentionally changed, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3015

Message

```
AUDIT, <timestamp>, [SEC-3015], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Moved RADIUS server
<Server name> to position <New position>.
```

Probable cause

Indicates that a user has changed the position of the remote authentication dial-in user service (RADIUS) server.

Recommended action

Verify that the RADIUS server position was intentionally changed. If the RADIUS server position was intentionally changed, no action is required. If the RADIUS server position was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3016

Message

```
AUDIT, <timestamp>, [SEC-3016], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Attribute
[<Attribute Name>] of RADIUS server <server ID> changed
<Attribute related info, if any>.
```

Probable cause

Indicates that a user has changed the specified attribute of the remote authentication dial-in user service (RADIUS) server.

Recommended action

Verify that the RADIUS attribute was intentionally changed. If the RADIUS attribute was intentionally changed, no action is required. If the RADIUS attribute was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3017

Message

```
AUDIT, <timestamp>, [SEC-3017], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Event Related
Info>.
```

Probable cause Indicates that a user has changed the remote authentication dial-in user service (RADIUS) configuration.

Recommended action Verify that the RADIUS configuration was intentionally changed. If the RADIUS configuration was intentionally changed, no action is required. If the RADIUS configuration was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3018

Message

```
AUDIT, <timestamp>, [SEC-3018], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Parameter
[<Parameter Name>] changed from [<Old Value>] to [<New
Value>].
```

Probable cause Indicates that the specified **passwdCfg** parameter is changed.

Recommended action Verify that the **passwdCfg** parameter was intentionally changed. If the **passwdCfg** parameter was intentionally changed, no action is required. If the **passwdCfg** parameter was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3019

Message

```
AUDIT, <timestamp>, [SEC-3019], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Passwdcfg parameters
set to default values.
```

Probable cause Indicates that the **passwdCfg** parameters are set to default values.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3020

Message

```
AUDIT, <timestamp>, [SEC-3020], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Successful login
attempt via <connection method and IP Address>.
```

Probable cause

Indicates that a successful login occurred. An IP Address is displayed when the login occurs over a remote connection.

Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3021

Message

```
AUDIT, <timestamp>, [SEC-3021], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Failed login attempt
via <connection method and IP Address>.
```

Probable cause

Indicates that a failed login attempt occurred.

Recommended action

Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3022

Message

```
AUDIT, <timestamp>, [SEC-3022], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Successful logout by
user [<User>].
```

Probable cause

Indicates that the specified user has successfully logged out.

Recommended action

No Action is Required.

Severity INFO

SEC-3023

Message

```
AUDIT, <timestamp>, [SEC-3023], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: failed, Info: Account [<User>]
locked, failed password attempts exceeded.
```

Probable cause Indicates that failed password attempts exceeded, the account has been locked.

Recommended action The Account may automatically unlock after the lockout duration has expired or an administrator may manually unlock the account.

Severity INFO

SEC-3024

Message

```
AUDIT, <timestamp>, [SEC-3024], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: User account [<User
Name>], password changed.
```

Probable cause Indicates that the user's password changed.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3025

Message

```
AUDIT, <timestamp>, [SEC-3025], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: User account [<User
Name>] added. Role: [<Role Type>], Password [<Password
Expired or not>], Home AD [<Home AD>], AD list [<AD
membership List>].
```

Probable cause Indicates a new user account was created.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3026

Message

```
AUDIT, <timestamp>, [SEC-3026], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: User account [<User
Name>], role changed from [<Old Role Type>] to [<New Role
Type>].
```

Probable cause Indicates that user account role was changed.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3027

Message

```
AUDIT, <timestamp>, [SEC-3027], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: User account [<User
Name>] [<Changed Attributes>].
```

Probable cause Indicates that user account properties were changed.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3028

Message

```
AUDIT, <timestamp>, [SEC-3028], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: User account [<User
Name>] deleted.
```

Probable cause Indicates that the specified user account was deleted.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3029

Message

```
AUDIT, <timestamp>, [SEC-3029], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Backup user account
\"<User Account Name>\" recovered.
```

Probable cause Indicates that back user accounts were recovered.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3030

Message

```
AUDIT, <timestamp>, [SEC-3031], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info:<Event Specific Info>
```

Probable cause Indicates the specified **secCertUtil** operation was performed.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3031

Message

```
AUDIT, <timestamp>, [SEC-3031], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Distributed<List of
Databases> db(s) to <Number of domains> domain(s),
dom-id(s)<List of Domains>.
```

Probable cause Indicates that the specified event has occurred.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3032

Message

```
AUDIT, <timestamp>, [SEC-3032], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Switch is configured
to <accept or reject> <Database name> database.
```

Probable cause Indicates that the specified event has occurred to accept or reject a certain database.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3033

Message

```
AUDIT, <timestamp>, [SEC-3033], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
fddcfg --fabwideset, Status: success, Info: Fabric wide
configuration set to <Fabric-wide configuration set by
user>.
```

Probable cause Indicates that the specified event has occurred.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3034

Message

```
AUDIT, <timestamp>, [SEC-3034], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
aaaconfig, Status: success, Info: Authentication
configuration changed from <Previous Mode> to <Current
Mode>.
```

Probable cause Indicates that an authentication configuration has changed.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3035

Message

```
AUDIT, <timestamp>, [SEC-3035], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
ipfilter, Status: success, Info: <IP Filter Policy> IP
filter policy(ies) saved.
```

Probable cause Indicates that the specified IP filter policy(ies) have been saved.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3036

Message

```
AUDIT, <timestamp>, [SEC-3036], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
ipfilter, Status: failed, Info: Failed to save changes
for <IP Filter Policy> ipfilter policy(s).
```

Probable cause Indicates that the specified IP filter policy(ies) have not been saved.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3037

Message

```
AUDIT, <timestamp>, [SEC-3037], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
ipfilter, Status: success, Info: <IP Filter Policy>
ipfilter policy activated.
```

Probable cause Indicates that the specified IP filter policy has been activated.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3038

Message

```
AUDIT, <timestamp>, [SEC-3038], INFO, SECURITY,
<event-initiator-details>, <event-location>, , Event:
ipfilter, Status: failed, Info: Failed to activate <IP
Filter Policy>.
```

Probable cause Indicates that the specified IP filter policy failed to activate.

Recommended action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3039

Message `AUDIT, <timestamp>, [SEC-3039], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: Securty Violation, Status: failed, Info: Unauthorized host with IP address <IP address of the violating host> tries to establish connection using <Protocol Connection Type>.`

Probable cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended action Check for unauthorized access to the switch through the specified protocol connection. Take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3040

Message `AUDIT, <timestamp>, [SEC-3040], WARNING, <Key> [ <Feature> license ] going to expire in <Expiry_days> day(s).`

Probable Cause Indicates that the license period will expire soon.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-3041

Message `AUDIT, <timestamp>, [SEC-3041], WARNING, <Key> [ <Feature> license ] is expired.`

Probable Cause Indicates that the license period has expired.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-3044

Message `AUDIT, <timestamp>, [SEC-3044], INFO, SECURITY, <event-initiator-details>, <event-location>, FIPS mode has been changed to <Fips Mode>.`

Probable Cause Indicates that there was a change in the FIPS mode.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3045

Message `AUDIT, <timestamp>, [SEC-3045], INFO, SECURITY, <event-initiator-details>, <event-location>, System has been zeroized.`

Probable Cause Indicates that the system has been zeroized.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3046

Message `AUDIT, <timestamp>, [SEC-3046], INFO, SECURITY, <event-initiator-details>, <event-location>, FIPS self tests mode has been set to <Self Test Mode>.`

Probable Cause Indicates that there was a change in the FIPS Self Test mode.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3047

Message `AUDIT, <timestamp>, [SEC-3047], INFO, SECURITY, <event-initiator-details>, <event-location>, RBAC permission denied for CLI : <Cmd Name>.`

Probable Cause Indicates that the user does not have permission to execute this command.

Recommended Action Verify that the user has the required permission to execute this command.

Severity INFO

SEC-3048

Message `AUDIT, <timestamp>, [SEC-3048], INFO, SECURITY, <event-initiator-details>, <event-location>, FIPS mode has been enabled in the system using force option.`

Probable Cause Indicates that the system has been forced to FIPS mode.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3049

Message `AUDIT, <timestamp>, [SEC-3049], INFO, SECURITY, <event-initiator-details>, <event-location>, Status of bootprom access is changed using fipscfg CLI to : <Access Status>.`

Probable Cause Indicates that the status of bootprom access is changed using the **fipscfg** command.

Recommended Action No action is required.

Severity INFO

SEC-3050

Message

```
AUDIT, <timestamp>, [SEC-3050], INFO, SECURITY, Event:
<Event Name>, Status: success, Info: <Event Specific
Info>.
```

Probable Cause

Indicates that the specified **sshutil** operation was performed.

Recommended Action

Verify if the security event was planned, if yes then no action is required else take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3051

Message

```
AUDIT, <timestamp>, [SEC-3051], INFO, SECURITY,
<event-initiator-details>, <event-location>, , The
license key <key> is <Action>.
```

Probable Cause

Indicates that a license key is added or removed

.Recommended Action

No action is required.

Severity

INFO

102

AUDIT SNMP System Messages

This chapter contains information on the following AUDIT SNMP messages:

- SNMP-1004 878
- SNMP-1005 878
- SNMP-1006 878

SNMP-1004

Message `AUDIT, <timestamp>, [SNMP-1004], ERROR, CONFIGURATION, <event-initiator-details>, <event-location>, , Incorrect SNMP configuration.`

Probable cause Indicates that the simple network management protocol (SNMP) configuration s incorrect and the SNMP service will not work correctly.

Recommended action Reset the SNMP configuration to default.

Severity ERROR

SNMP-1005

Message `AUDIT, <timestamp>, [SNMP-1005], INFO, CONFIGURATION, <event-initiator-details>, <event-location>, , SNMP configuration attribute, <Changed attribute>, has changed from <Old Value> to <New Value>`

Probable cause Indicates that the simple network management protocol (SNMP) configuration has changed as indicated. The parameter that was modified is displayed as well as the old and new values for that parameter.

Recommended action Execute the **snmpConfig --show** command to display the new configuration.

Severity INFO

SNMP-1006

Message `AUDIT, <timestamp>, [SNMP-1006], INFO, CONFIGURATION, <event-initiator-details>, <event-location>, , <SNMP Configuration group> configuration was reset to default.`

Probable cause Indicates that the simple network management protocol (SNMP) configuration group was reset to the factory default.

Recommended action Execute the **snmpConfig --show** command to display the new group configuration.

Severity INFO

103

AUDIT SULB System Messages

This chapter contains information on the following AUDIT SULB messages:

- SULB-1001 898
- SULB-1002 898
- SULB-1003 898
- SULB-1004 899
- SULB-1009 899
- SULB-1010 907
- SULB-1017 908
- SULB-1018 908
- SULB-1020 909
- SULB-1021 909
- SULB-1023 910
- SULB-1024 910
- SULB-1026 911
- SULB-1030 911
- SULB-1031 912
- SULB-1032 912
- SULB-1033 912
- SULB-1034 913
- SULB-1035 913
- SULB-1037 914

SULB-1001

Message

```
AUDIT, <timestamp>, [SULB-1001], WARNING, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwaredownload command has started.
```

Probable cause

Indicates that the **firmwareDownload** command has been entered. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended action

No action is required. Allow the **firmwareDownload** command to continue without disruption. Do not fail over or power down the system during firmware upgrade.

Run the **firmwareDownloadStatus** command for more information.

Severity

WARNING

SULB-1002

Message

```
AUDIT, <timestamp>, [SULB-1002], INFO, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwaredownload command has completed successfully.
```

Probable cause

Indicates that the **firmwareDownload** command has completed successfully and switch firmware has been updated.

Recommended action

No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information. Run **firmwareShow** to verify the firmware versions.

Severity

INFO

SULB-1003

Message

```
AUDIT, <timestamp>, [SULB-1003], INFO, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwarecommit has started.
```

Probable cause

Indicates that the **firmwareCommit** command has been entered.

Recommended action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1004

Message

```
AUDIT <timestamp>, [SULB-1004], INFO, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwarecommit has completed.
```

Probable Cause Indicates that the **FirmwareCommit** command is executed.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1009

Message

```
AUDIT, <timestamp>, [SULB-1009], INFO, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwaredownload command failed. status: 0x<status code>,
error: 0x<error code>.
```

Probable cause Indicates that the **firmwareDownload** command failed. The additional *status code* and *error code* provide debugging information.

Table 9 lists **firmwareDownload** status messages and status codes. Some of them will not show up in this RASLOG message. They are listed for the sake of completeness.

Table 9 Status messages and status codes (1 of 5)

Status message	Status code
"**firmwareDownload** sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because **firmwareDownload** is already in progress."	0x32
"Sanity check failed because FABRIC OS is disabled on Active CP."	0x33
"Sanity check failed because HAMD is disabled on Active CP."	0x34

Table 9 Status messages and status codes (2 of 5)

Status message	Status code
“Sanity check failed because **firmwareDownload** is already in progress.”	0x35
"Sanity check failed because FABRIC OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
“**firmwareDownload** failed on Standby CP.”	0x40
“**firmwareDownload** failed on Standby CP.”	0x41
“**firmwareDownload** failed on Standby CP.”	0x42
“**firmwareCommit** failed on Standby CP.”	0x43
“**firmwareDownload** failed.”	0x44
“**firmwareDownload** failed due to IPC error.”	0x50
"Unable to check the firmware version on Standby CP due to IPC error."	0x51
“**firmwareDownload** failed due to IPC error.”	0x52
“**firmwareDownload** failed due to IPC error.”	0x53
"Standby CP failed to reboot due to IPC error."	0x54
“**firmwareCommit** operation failed due to IPC error.”	0x55
"Unable to check the firmware version on Standby CP due to IPC error."	0x56
“Unable to restore the original firmware due to Standby CP timeout.”	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on Standby CP due to IPC error."	0x59
“Sanity check failed because **firmwareDownload** is already in progress.”	0x60
“Sanity check failed because **firmwareDownload** is already in progress.”	0x61
NOT USED	0x62
"System Error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Active and Standby CP failed to gain HA synchronization within 10 minutes."	0x66

Table 9 Status messages and status codes (3 of 5)

Status message	Status code
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
"**firmwareCommit** has started to restore the secondary partition."	0x69
"Local CP is restoring its secondary partition."	0x6a
"Unable to restore the secondary partition. Please use **firmwareDownloadStatus** and **firmwareShow** to see firmware status."	0x6b
"**firmwareDownload** has started on Standby CP. It might take up to 10 minutes."	0x6c
"**firmwareDownload** has completed successfully on Standby CP."	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
"**firmwareDownload** has completed successfully on Standby CP."	0x72
"**firmwareDownload** has started on Standby CP. It might take up to 10 minutes."	0x73
"**firmwareDownload** has completed successfully on Standby CP."	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
"**firmwareCommit** has started on Standby CP."	0x77
"**firmwareCommit** has completed successfully on Standby CP."	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
"**firmwareCommit** has started on both Active and Standby CPs."	0x7b
"**firmwareCommit** has completed successfully on both CPs."	0x7c
"**firmwareCommit** failed on Active CP."	0x7d
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f

Table 9 Status messages and status codes (4 of 5)

Status message	Status code
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
“There was an unexpected reboot during **firmwareDownload**. The command is aborted.”	0x84
"Standby CP was not responding. The command is aborted."	0x85
“**firmwareCommit** has started on both CPs. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x86
“**firmwareCommit** has started on the local CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x87
“**firmwareCommit** has started on the remote CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x88
“Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status.”	0x89
“**firmwareDownload** command has completed successfully.”	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
“**firmwareDownload** has started.”	0x8f
“**firmwareCommit** has started.”	0x90
“**firmwareDownload** has completed successfully.”	0x91
“**firmwareCommit** has completed successfully.”	0x92
“**firmwareCommit** has started to restore the secondary partition.”	0x93
“**firmwareCommit** failed.”	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
“**firmwareDownload** timed out.”	0xa1

Table 9 Status messages and status codes (5 of 5)

Status message	Status code
“Reboot occurred during **firmwareDownload**. **firmwareCommit** will be started to recover the blade.”	0xa2
“Blade rebooted during **firmwareCommit**. The operation will be restarted.”	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5
“New firmware failed to boot up. Please retry **firmwareDownload**.”	0xa6
“**firmwareCommit** has started on the blade. This may take up to 10 minutes.”	0xa7
“**firmwareRestore** is entered. System will reboot and a **firmwareCommit** operation will start upon boot up.”	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
“Blade failed to reboot with the original image. **firmwareRestore** command failed.”	0xac

Table 10 lists additional **firmwareDownload** error messages and error codes. They provide more details on why **firmwareDownload** failed.

Table 10 Error messages and error codes (1 of 3)

Error message	Error code
"Image is up-to-date. No need to download the same version of firmware."	0xF
“Upgrade is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x10
“OSRootPartition is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding. For example: swap OSRootPartitions and reboot.”	0x11
“Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check **firmwareDownload** help page for other possible failure reasons.”	0x12
"The RPM package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package."	0x15

Table 10 Error messages and error codes (2 of 3)

Error message	Error code
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
“Error in getting lock device for **firmwareDownload**.”	0x18
“Error in releasing lock device for **firmwareDownload**.”	0x19
“**firmwareCommit** failed.”	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
“OSLoader is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x1d
“New image has not been committed. Run **firmwareCommit** or **firmwareRestore** first and then try **firmwareDownload**.”	0x1e
“**firmwareRestore** failed.”	0x1f
"Both images are mounted to the same device."	0x20
“Unable to unionist old packages.”	0x21
“**firmwareDownload** is already in progress.”	0x22
“**firmwareDownload** timed out.”	0x23
"Our of disk space."	0x24
“Primary filesystem is inconsistent. Run **firmwareRestore** to restore the original firmware, or contact your service provider for recovery.”	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Please contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
“The platform option is not supported. Run **chassisConfig** to reset the option first and then try **firmwareDownload**.”	0x2a
"Failed to install RPM package."	0x2b

Table 10 Error messages and error codes (3 of 3)

Error message	Error code
"Cannot downgrade directly to this version. Downgrade to an intermediate version first and then download the desired version."	0x2c
“Cannot download 5.1 because Device Based Routing policy is not supported by 5.1. Use **aptPolicy** to change the routing policy before proceeding.”	0x2d
"Invalid RPM package. Please reload firmware packages on the file server."	0x2e
"Cannot downgrade due to presence of blade type 17. Remove or power off these blades before proceeding."	0x2f
"Cannot downgrade due to presence of blade type 24. Remove or power off these blades before "	0x30
"Cannot downgrade due to presence of long-distance ports in LS mode. Please remove these settings before proceeding."	0x31
"Network is not reachable. Please verify the IP address of the server is correct."	0x32

The following section explains the causes of some common error messages:

0x15 - Failed to download Red Hat package manager (RPM) package. If this error occurs immediately after **firmwareDownload** is started, the firmware on the switch may be two releases older than the requested firmware. **firmwareDownload** supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number, for example, X.Y). The following are major upgrade versions for the Fabric OS: v4.0, v4.1, v4.2, v4.4, v5.0, v5.1, 5.2, and 5.3. In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of **firmwareDownload**, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmwareDownload** command. If the problem persists, contact your system administrator.

0x18 - Error in getting lock device for **firmwareDownload**. This error may occur because another **firmwareDownload** is already in progress. Run **firmwareDownloadStatus** to verify that this is the case. Wait for the current session to finish before proceeding.

0x23 - **firmwareDownload** timed out. This error may occur because **firmwareDownload** has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.

0x24 - out of disk space. This error may occur because some coredump files have not been removed from the filesystem and are using up disk space. Remove these coredump files using the **supportSave** command before proceeding.

0x29 - The pre-install script failed. This error may be caused by an unsupported blade type in the chassis. Remove or power off the unsupported blades before proceeding. Another possible cause may be an invalid **chassisConfig** option setting. In that case, reset the **chassisConfig** option before retrying **firmwareDownload**.

0x2e - Invalid Red Hat package manager (RPM) package. This error maybe caused by an inconsistent firmware image loaded on the file server. It may also be caused by temporary networking issues. Please reload firmware packages on the file server, then retry **firmwareDownload**. If the problem persists, contact your system administrator.

Table 11 lists the **firmwareDownload** state names and state values. They indicate where in the **firmwareDownload** process the error occurred.

Table 11 Upgrade state and code value (1 of 2)

Upgrade state	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c

Table 11 **Upgrade state and code value (2 of 2)**

Upgrade state	Code
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended action

Run the **firmwareDownloadStatus** command for more information.

In a director-class switch, when **firmwareDownload** fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another **firmwareDownload**.

In a director-class switch, when **firmwareDownload** fails, the two CPs may end up with different versions of firmware and they may not gain high-availability (HA) sync. In that case, run **firmwareDownload** single mode (-s) to upgrade the firmware on the standby CP to the same version as the active CP. Then retry **firmwareDownload** to download the desired version of firmware onto the CPs.

Refer to the *EMC Connectrix B Series Fabric OS Administrator's Guide* for troubleshooting information.

Severity

INFO

SULB-1010

Message

```
AUDIT, <timestamp>, [SULB-1010], INFO, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwarecommit failed (status=0x<error code>).
```

Probable cause Indicates that the **firmwareCommit** failed. The error code provides debugging information. See Table 10 on page 903 for more information.

Recommended action If the failure is caused by an inconsistent filesystem, contact the EMC Customer Support Center.

Severity INFO

SULB-1017

Message

```
AUDIT, <timestamp>, [SULB-1017], ERROR, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwaredownload failed in slot <Slot number>.
```

Probable cause Indicates that **firmwareDownload** failed in the specified blade. The error may be caused by an inconsistent AP blade firmware stored on the active CP. It may also caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended action Run the **slotShow** command. If the blade is in FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload** to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact the EMC Customer Support Center.

Severity ERROR

SULB-1018

Message

```
AUDIT, <timestamp>, [SULB-1018], ERROR, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwaredownload timed out in slot <Slot number>.
```

Probable cause The error may be caused by a blade initialization issue after the new firmware is downloaded and the blade is rebooted. The error may also be caused by an internal Ethernet issue or by a persistent storage failure.

Recommended action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload**. If the blade is stuck in LOADING state, remove

and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact the EMC Customer Support Center.

Severity ERROR

SULB-1020

Message

```
AUDIT, <timestamp>, [SULB-1020], ERROR, FIRMWARE,
<event-initiator-details>, <event-location>, , New
firmware failed to boot in slot <Slot number>.
```

Probable cause The BP blade should reboot with the new image, but is still running the old image. This error may indicate that the new image has not been loaded correctly to the specified blade.

Recommended action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload** to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact the EMC Customer Support Center.

Severity ERROR

SULB-1021

Message

```
AUDIT, <timestamp>, [SULB-1021], WARNING, FIRMWARE,
<event-initiator-details>, <event-location>, , Firmware
is being downloaded to the blade in slot <Slot number>.
```

Probable cause Indicates that the firmware is being loaded to the specified blade.

Recommended action Run the **firmwareDownloadStatus** command to monitor the **firmwareDownload** progress. After it finishes, run the **firmwareShow** command to verify the firmware versions.

Severity WARNING

SULB-1023

Message

```
AUDIT, <timestamp>, [SULB-1023], WARNING, FIRMWARE,
<event-initiator-details>, <event-location>, , The blade
in slot <Slot number> has rebooted during
firmwaredownload.
```

Probable cause

The error may be caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering off and on of the indicated BP blade in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended action

firmwareCommit will be started automatically after the blade boots up to repair the secondary partition. If at the end of **firmwareCommit**, the blade firmware version is still inconsistent with the active CP firmware, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact the EMC Customer Support Center.

Severity

WARNING

SULB-1024

Message

```
AUDIT, <timestamp>, [SULB-1024], WARNING, FIRMWARE,
<event-initiator-details>, <event-location>, , Firmware
commit has completed on the blade in slot <Slot number>.
```

Probable cause

Indicates that the **firmwareCommit** operation has completed on the specified blade.

Recommended action

Run the **firmwareShow** command to verify the firmware versions. If the blade firmware is the same as the active CP firmware, **firmwareDownload** has completed successfully on the blade. However, if the **firmwareCommit** operation has been started to repair the secondary partition, at the end of **firmwareCommit**, the blade firmware version may still be inconsistent with the active CP firmware. In that case, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress.

Severity

WARNING

SULB-1026

Message

```
AUDIT, <timestamp>, [SULB-1026], WARNING, FIRMWARE,
<event-initiator-details>, <event-location>, , Firmware
commit operation started on the blade in slot <Slot
number>.
```

Probable cause

firmwareCommit has started on the specified blade. The operation may be a normal part of **firmwareDownload**, or it may have started to repair the secondary partition of the blade if the secondary partition is corrupted.

Recommended action

Wait for the commit operation to complete.

Severity

WARNING

SULB-1030

Message

```
AUDIT, <timestamp>, [SULB-1030], WARNING, FIRMWARE,
<event-initiator-details>, <event-location>, , The switch
has rebooted during relocating the internal firmware
image.
```

Probable cause

The error may be caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering the switch off and on in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended action

firmwareDownload will continue after the switch has rebooted. Run the **firmwareDownloadStatus** command to monitor progress. If the problem persists, contact the EMC Customer Support Center.

Severity

WARNING

SULB-1031

Message `AUDIT, <timestamp>, [SULB-1031], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , The switch is relocating an internal firmware image.`

Probable cause Indicates that the switch has rebooted with the new firmware and is relocating the AP firmware.

Recommended action Wait for the operation to complete.

Severity WARNING

SULB-1032

Message `AUDIT <timestamp>, [SULB-1032], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Relocating an internal firmware image on the CP.`

Probable cause Indicates that the switch has started firmware download to the co-CPU.

Recommended action Wait for the operation to complete.

Severity WARNING

SULB-1033

Message `AUDIT, <timestamp>, [SULB-1033], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Switch has completed relocating the internal firmware image.`

Probable cause Indicates that the **firmwareDownload** process has completed normally on the switch.

Recommended action Run the **firmwareShow** command to verify the firmware versions. Run the **switchShow** command to make sure the switch is enabled.

Severity WARNING

SULB-1034

Message

```
AUDIT, <timestamp>, [SULB-1034], ERROR, FIRMWARE,
<event-initiator-details>, <event-location>, ,
Firmwaredownload timed out.
```

Probable cause

The error may be caused by a switch initialization issue after the internal image is relocated. It may also be caused by an internal Ethernet issue or by persistent storage failure.

Recommended action

Reboot the switch. This will cause the internal image to be relocated again. Use the **firmwareDownloadStatus** to monitor the progress. If the problem persists, contact the EMC Customer Support Center.

Severity

ERROR

SULB-1035

Message

```
AUDIT, <timestamp>, [SULB-1035], ERROR, FIRMWARE,
<event-initiator-details>, <event-location>, , An error
has occurred relocation of the internal image.
```

Probable cause

Indicates that an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by the internal Ethernet or persistent storage hardware failure.

Recommended action

Reset the switch. This will cause the internal image to be relocated again. If the problem persists, contact the EMC Customer Support Center.

Severity

ERROR

SULB-1037

Message

```
AUDIT, <timestamp>, [SULB-1037], ERROR, FIRMWARE,
<event-initiator-details>, <event-location>, , HCL
failed. Reboot the switch manually using the reboot
command. However, it will disrupt the FC traffic.
```

Probable cause

Many reasons can cause HCL to fail, such as domain not confirmed.

Recommended action

Run the **reBoot** command to reboot the switch manually.

Severity

Error

104

AUDIT SWCH System Messages

This chapter contains information on the following AUDIT AUTH messages:

- SWCH-1012 900
- SWCH-1013 900
- SWCH-1014 900

SWCH-1012

Message

```
AUDIT, <timestamp>, [SWCH-1012], INFO, CFG,
<event-initiator-details>, <event-location>, , Trunk Area
(<trunk area>) has been enabled for one or more ports.
```

Probable Cause Indicates a Trunk Area has been enabled for one or more ports and the config file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1013

Message

```
AUDIT, <timestamp>, [SWCH-1013], INFO, CFG,
<event-initiator-details>, <event-location>, , Trunk Area
has been disabled for one or more ports.
```

Probable Cause Indicates Trunk Area assignment has been disabled for one or more ports and the config file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1014

Message

```
AUDIT, <timestamp>, [SWCH-1014], INFO, CFG,
<event-initiator-details>, <event-location>, , All Trunk
Areas have been disabled.
```

Probable Cause Indicates all Trunk Areas have been disabled and the config file has been updated.

Recommended Action No action is required.

Severity INFO

105

AUDIT UCST System Messages

This chapter contains information on the following AUDIT AUTH messages:

- UCST-1021 904
- UCST-1022 904
- UCST-1023 904
- UCST-1024 905
- UCST-1025 905
- UCST-1026 905
- UCST-1027 906

UCST-1021

Message

```
AUDIT, <timestamp>, [UCST-1021], INFO, CFG,
<event-initiator-details>, <event-location>, , In-order
delivery option has been enabled.
```

Probable Cause Indicates the IOD option has been enabled for the switch. This option guarantees in-order delivery of frames during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1022

Message

```
AUDIT, <timestamp>, [UCST-1022], INFO, CFG,
<event-initiator-details>, <event-location>, , In-order
delivery option has been disabled.
```

Probable Cause Indicates the IOD option has been disabled for the switch. This may cause out-of-order delivery of frames.

Recommended Action No action is required.

Severity INFO

UCST-1023

Message

```
AUDIT, <timestamp>, [UCST-1023], INFO, CFG,
<event-initiator-details>, <event-location>, , Dynamic
Load Sharing option has been enabled.
```

Probable Cause Indicates the DLS option has been enabled for the switch. This will move existing routes to a new redundant path, when this path becomes available.

Recommended Action No action is required.

Severity INFO

UCST-1024

Message

```
AUDIT, <timestamp>, [UCST-1024], INFO, CFG,
<event-initiator-details>, <event-location>, , Dynamic
Load Sharing option has been disabled.
```

Probable Cause Indicates the DLS option has been disabled for the switch.

Recommended Action No action is required.

Severity INFO

UCST-1025

Message

```
AUDIT, <timestamp>, [UCST-1025], INFO, CFG,
<event-initiator-details>, <event-location>, , In-order
delivery option has been enabled with Lossless-DLS
option.
```

Probable Cause Indicates the IOD option has been enabled for the switch. This option guarantees in-order delivery of frames during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1026

Message

```
AUDIT, <timestamp>, [UCST-1026], INFO, CFG,
<event-initiator-details>, <event-location>,
,LossLess-DLS option has been enabled.
```

Probable Cause Indicates that the NoFrameDrop option is enabled. This will help minimizing frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1027

Message

```
AUDIT, <timestamp>, [UCST-1027], INFO, CFG,
<event-initiator-details>, <event-location>, ,
LossLess-DLS option has been disabled.
```

Probable Cause

Indicates that the NoFrameDrop option is disabled. This may cause higher frame loss during topology changes.

Recommended Action

No action is required.

Severity

INFO

106

AUDIT ZONE System Messages

This chapter contains information on the following AUDIT ZONE messages:

- ZONE-3001 908
- ZONE-3002 908
- ZONE-3003 909
- ZONE-3004 909
- ZONE-3005 910
- ZONE-3006 910
- ZONE-3007 910
- ZONE-3008 911
- ZONE-3009 911
- ZONE-3010 911
- ZONE-3011 912
- ZONE-3012 912
- ZONE-3013 912
- ZONE-3014 913
- ZONE-3015 913
- ZONE-3016 914
- ZONE-3017 914
- ZONE-3018 914
- ZONE-3019 915
- ZONE-3020 915
- ZONE-3021 916
- ZONE-3022 916
- ZONE-3023 916
- ZONE-3024 917
- ZONE-3025 917

ZONE-3001

Message

```
AUDIT, <timestamp>, [ZONE-3001], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Zone object type>
\"<Zone object member list>\" added to <Zone object set
type> \"<Zone object set name>\".
```

Probable cause

Indicates that a new zone object member or members have been added to the specified zone object set.

The *zone object type* can be "alias", "zone member", "zone" or "zone configuration". The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3002

Message

```
AUDIT, <timestamp>, [ZONE-3002], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Zone object set
type> \"<Zone object set name>\" created with <Zone
object type> \"<Zone object member list>\".
```

Probable cause

Indicates that a new zone object set was created and the specified zone object member or members were added to that new zone object set.

The *zone object type* can be "alias", "zone member", "zone" or "zone configuration". The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3003

Message

```
AUDIT, <timestamp>, [ZONE-3003], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Zone object type>
\"<Zone object name>\" deleted.
```

Probable cause

Indicates that the specified zone object has been deleted.

The *zone object type* can be “alias”, “zone member”, “zone” or “zone configuration”. The string “...” appears at the end of the zone object member list if the list was truncated in the message.

Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3004

Message

```
AUDIT, <timestamp>, [ZONE-3004], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Zone object type>
\"<Zone object member list>\" removed from <Zone object
set type> \"<Zone object set name>\".
```

Probable cause

Indicates that the specified zone object member or members have been removed from the specified zone object set.

The *zone object type* can be “alias”, “zone member”, “zone” or “zone configuration”. The string “...” appears at the end of the zone object member list if the list was truncated in the message.

Recommended action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

ZONE-3005

Message

```
AUDIT, <timestamp>, [ZONE-3005], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: All zone information
cleared from transaction buffer.
```

Probable cause Indicates that all zone information has been cleared from the transaction buffer.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3006

Message

```
AUDIT, <timestamp>, [ZONE-3006], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Current zone
configuration disabled. <AD Id>.
```

Probable cause Indicates that the current zone configuration has been disabled.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3007

Message

```
AUDIT, <timestamp>, [ZONE-3007], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Zone configuration
\"<Zone configuration>\" enabled. <AD Id>.
```

Probable cause Indicates that the specified zone configuration has been enabled.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3008

Message

```
AUDIT, <timestamp>, [ZONE-3008], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Current zone
configuration saved to MRAM. <AD Id>.
```

Probable cause Indicates that the current zone configuration has been successfully saved to magnetoresistive random access memory (MRAM).

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3009

Message

```
AUDIT, <timestamp>, [ZONE-3009], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Event Description>.
```

Probable cause Indicates that the specified zone transaction has been aborted.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3010

Message

```
AUDIT, <timestamp>, [ZONE-3010], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Zone object \"<Zone
object name>\" copied to new zone object \"<New Zone
object name>\".
```

Probable cause Indicates that the specified zone object has been copied to a new zone object.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3011

Message

```
AUDIT, <timestamp>, [ZONE-3011], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Zone object \"<Zone
object name>\" expunged.
```

Probable cause Indicates that the specified zone object has been expunged.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3012

Message

```
AUDIT, <timestamp>, [ZONE-3012], INFO, ZONE,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Zone object \"<Zone
object name>\" renamed to \"<New Zone object name>\".
```

Probable cause Indicates that the specified zone object has been renamed.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3013

Message

```
AUDIT, <timestamp>, [ZONE-3013], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <Admin domain name>
has been activated.
```

Probable cause Indicates that the specified admin domain (AD) has been activated.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3014

Message

```
AUDIT, <timestamp>, [ZONE-3014], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: \"<AD object member
list>\" added to <AD object set type> \"<AD object set
name>\".
```

Probable cause Indicates that the specified new admin domain (AD) object member or members have been added to the specified AD object set.

An *AD object set type* is "AD member". The string "..." appears at the end of the AD object member list if the list was truncated in the message.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3015

Message

```
AUDIT, <timestamp>, [ZONE-3015], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: AD configurations
applied.
```

Probable cause Indicates that the current admin domain (AD) configuration has been saved to flash is being enforced.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3016

Message

```
AUDIT, <timestamp>, [ZONE-3016], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: All AD definitions
cleared.
```

Probable cause Indicates that all admin domain (AD) definitions and all zone configurations under them have been cleared.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3017

Message

```
AUDIT, <timestamp>, [ZONE-3017], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <AD object set type>
\"<AD object set name>\" created with \"<AD object member
list>\".
```

Probable cause Indicates that the specified admin domain (AD) has been created.

An *AD object set type* is "AD member". The string "..." appears at the end of the AD object member list if the list was truncated in the message.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3018

Message

```
AUDIT, <timestamp>, [ZONE-3018], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <AD object name> has
been deactivated.
```

Probable cause Indicates that the specified admin domain (AD) object has been deactivated.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3019

Message

```
AUDIT, <timestamp>, [ZONE-3019], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: <AD object type>
\"<AD object name>\" deleted.
```

Probable cause Indicates that the specified admin domain (AD) object has been deleted.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3020

Message

```
AUDIT, <timestamp>, [ZONE-3020], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: \"<AD object member
list>\" removed from <AD object set type> \"<AD object
set name>\".
```

Probable cause Indicates that the specified admin domain (AD) member or members have been removed from an AD.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3021

Message

```
AUDIT, <timestamp>, [ZONE-3021], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: AD object \"<AD
object name>\" renamed to \"<New AD object name>\".
```

Probable cause Indicates that the specified admin domain (AD) has been renamed.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3022

Message

```
AUDIT, <timestamp>, [ZONE-3022], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: success, Info: Current AD
configuration saved to flash.
```

Probable cause Indicates that the current admin domain (AD) configuration has been saved to flash.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3023

Message

```
AUDIT, <timestamp>, [ZONE-3023], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Event:
<Event Name>, Status: Failure, Info: AD Apply operation
failed due to transaction conflict.
```

Probable cause Indicates that the admin domain **ad --apply** operation failed due to a transaction conflict.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3024

Message

```
AUDIT, <timestamp>, [ZONE-3024], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Command:
<Command Name>, Status: success, Info: executed. <AD Id>.
```

Probable cause Indicates that the admin domain **ad --transabort** operation was successful in the specified AD.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3025

Message

```
AUDIT, <timestamp>, [ZONE-3025], INFO, FABRIC,
<event-initiator-details>, <event-location>, , Command:
<Command Name> Info: executed. In AD <AD Id>.
```

Probable cause Indicates that the admin domain **ad --exec** operation was executed in the specified AD.

Recommended action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO