

Oracle® Communications

Policy Management

Troubleshooting Reference

Release 12.5

E94271-02

December 2023

Policy Management Troubleshooting Reference, Release 12.5

E94271-02

Copyright © 2013, 2023, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Introduction.....	xxx
About this Guide.....	xxx
How This Guide Is Organized	xxx
Scope and Audience	xxx
Related Publications	xxx
Locate Product Documentation on the Oracle Help Center Site	xxx
Customer Training	xxx
My Oracle Support	xxx
Emergency Response.....	xxx
1 Incidents, Notifications, and Logs Overview	
About Incidents.....	1-1
About Notifications	1-1
About Logs.....	1-1
Viewing Policy Server Logs.....	1-2
Viewing the Trace Log	1-3
Syslog Support.....	1-5
The CMPP Log.....	1-5
The SMS Log	1-6
The SMPP Log.....	1-6
The SMTP Log.....	1-6
The HTTP Log.....	1-6
Configuring Log Settings for Servers in a Cluster.....	1-6
Activity Logs per Subscriber	1-11
2 Trace Log Notifications	
Expanded List.....	2-1
1 – BoD TraceLog Init	2-1
2 – OSSI Collector Conn Establish	2-2
3 – OSSI Collector Error.....	2-2
4 – OSSI Collector Start.....	2-3
5 – OSSI Collector End.....	2-3

6 – OSSI Collector Abort.....	2-4
7 – OSSI Collector Config Read Error.....	2-4
8 – OSSI Collector Connection Success	2-5
9 – OSSI Collector Connection Fail	2-5
10 – OSSI Collector No CMTS Nodes.....	2-6
11 – OSSI Collector No Subs for CMTS	2-6
12 – OSSI Collector Config Param Not Found	2-7
13 – OSSI Collector Validate Error	2-8
14 – DC Started	2-8
21 – Subnet SNMP Coll Task Start	2-9
22 – Subnet SNMP Coll Task Timeout.....	2-9
23 – Subnet SNMP Coll Task Error	2-10
24 – Subnet SNMP Coll Task Skip.....	2-10
25 – BOD Classifier Not Active	2-11
26 – BOD Classifier Active Exit Sub IP.....	2-11
38 – Subnet SNMP Collector Task Status.....	2-12
39 – Subnet SNMP Collector Task End.....	2-13
41 – DC SNMP Collector Start.....	2-13
42 – DC Collect Timeout.....	2-14
43 – DC Collect Error	2-14
44 – DC Empty Community.....	2-15
50 – BOD HTTP Request Success	2-15
58 – DC SNMP Collector Status	2-16
59 – DC SNMP Collector Stop	2-17
61 – SNMP Collector Task Start.....	2-17
62 – SNMP Timeout	2-18
63 – SNMP Error	2-18
64 – Invalid Cable Modem MAC	2-19
65 – Invalid Cable Modem IP	2-19
66 – Invalid CPE IP.....	2-20
68 – SNMP Community Empty.....	2-20
70 – BOD SOAP Request Failure.....	2-21
78 – SNMP Collector Task Status	2-22
79 – SNMP Collector Task End.....	2-22
80 – BOD SOAP Request Success.....	2-23
81 – DC CMTS Distributor Task Start.....	2-23
82 – DC CMTS Error.....	2-24
98 – DC CMTS Distributor Task Status	2-24
99 – DC CMTS Distributor Task Stop	2-25
100 – BOD Conn.....	2-25
101 – Sub Distributor Task Start	2-26
102 – Sub Distributor Task Delete Error.....	2-27
103 – Sub Distributor Task Update Error.....	2-27

104 – Sub Distributor Task Send Reconfig Error.....	2-28
105 – Sub Distributor Task Send Refresh Chann Error	2-28
106 – Sub Distributor Task Send Refresh Acct Error	2-29
107 – Sub Distributor Task Send Tier Error.....	2-29
108 – Sub Distributor Task Send Channel Error	2-30
118 – Sub Distributor Task Status.....	2-30
119 – Sub Distributor Task End	2-31
121 – OSSI Distributor Task Start	2-32
122 – OSSI Distributor Task Error	2-32
123 – OSSI Distributor Task Abort	2-33
124 – OSSI Distributor Task Remote MA Error.....	2-33
125 – OSSI Distributor Task Update Acct Error	2-34
126 – OSSI Distributor Task Update CMTS Error.....	2-34
127 – OSSI Distributor Task Update Tiers Error	2-35
128 – OSSI Distributor Task Update Entitle Error	2-35
139 – OSSI Distributor Task End	2-36
141 – CMTS MA Collector Task Start	2-37
142 – CMTS MA Collector Task Error	2-37
157 – CMTS MA Collector Task Status MAS.....	2-38
158 – CMTS MA Collector Task Status CMTS.....	2-38
159 – CMTS MA Collector Task End.....	2-39
161 – PCMM Dist Task Start.....	2-39
177 – PCMM Dist Task MPE Status	2-40
178 – PCMM Dist Task Status	2-40
179 – PCMM Dist Task End.....	2-41
180 – DC Manual Task Start	2-42
201 – Healthchecker Task Start	2-42
219 – Healthchecker Task End	2-43
220 – DC AlertAging Task Start.....	2-43
239 – DC AlertAging Task End.....	2-44
240 – OM Stats Task Start	2-44
241 – OM Stats Task Data Available.....	2-45
243 – OM Stats Task Missing MPE.....	2-45
244 – OM Stats Task Missing Stats	2-46
245 – OM Stats task Missing MPE DB	2-46
247 – OM Stats Task Retrieve Error.....	2-47
248 – OM Stats Task Retrieve Fail	2-48
249 – OM Stats Task Retrieve Incomplete	2-48
250 – OM Stats Task Proxy Fail.....	2-49
251 – OM Stats Task Retrieve Error2.....	2-49
252 – BoD DB Backup Fail.....	2-50
253 – BOD DB Backup Start	2-50
254 – BoD DB Backup End	2-51

256 – OM Stats Task Success	2-52
257 – OM Stats Task Warn	2-52
258 – OM Stats Task Failed.....	2-53
259 – OM Stats Task Finish.....	2-53
260 – BoD Cluster Reinit.....	2-54
261 – Bad WGET Status	2-54
276 – Stat Rsync Clean Task Success.....	2-55
278 – Stat Rsync Clean Task Failed	2-55
279 – Stat Rsync Cleanup Task Finish.....	2-56
280 – Subscription Aging Task Start	2-56
289 – Subscription Aging Task End	2-57
300 – BoD Send	2-57
301 – BoD Received Debug	2-58
302 – BoD Request Timed Out.....	2-59
303 – Quota Aging Task Start.....	2-59
304 – Quota Aging Task End.....	2-60
310 – BOD XML Syntax Error PCM	2-60
311 – BOD Missing Service Fields	2-61
312 – BOD XML Syntax Error	2-61
313 – BOD Service Index Exists	2-62
314 – BOD Same Service Mult Times.....	2-62
400 – BOD MAC Translate Conn Fail	2-63
401 – Stats Files Gen Task Start.....	2-63
402 – Stats File Gen Task Success	2-64
403 – Stats File Gen Task Failed.....	2-64
404 – Stats File Gen Task Finish.....	2-65
405 – Stats File Gen Task Not Execute	2-66
406 – Stats File Gen Task Fail Sync Blade.....	2-66
407 – Stats File Gen Task Fail Delete File	2-67
408 – Stats File Gen Task Fail NoStatsType.....	2-67
500 – BoD RDR Service Start Msg Received	2-68
501 – BoD RDR Unmapped Skip.....	2-68
502 – Stats Sync Task Success.....	2-69
503 – Stats Sync Task Fail.....	2-70
504 – Stats Sync Task End.....	2-70
505 – Stats Sync Task Repository Missing.....	2-71
506 – Stats Sync Task Repository Fail	2-71
507 – BoD Start Msg Processing Warn.....	2-72
508 – BOD RDR Parse Fail.....	2-72
509 – BoD Drop RDR Service.....	2-73
510 – BoD RDR Service Stop Msg Received	2-74
512 – BoD Drop RDR Bucket	2-74
513 – BoD RDR Unmapped Skip2.....	2-75

514 – BoD RDR Quota Msg Received	2-75
515 – BoD RDR Quota Msg Processing Warn Info Debug.....	2-76
550 – XML Request Initiated	2-76
552 – Account Send Error	2-77
553 – XML Export Results	2-77
554 – XML Export Failure.....	2-78
555 – XML Request Complete.....	2-78
620 – Push Init	2-79
621 – Push Done.....	2-80
625 – Subscriber Acct Start.....	2-80
626 – Subscriber Acct End	2-81
653 – RC Apply Change	2-81
1001 – CMTS Conn Lost Clear	2-82
1002 – CMTS Conn Lost	2-82
1003 – AM Conn Lost Clear	2-83
1004 – AM Conn Lost Set	2-84
1010 – PCMM Received AM	2-84
1011 – PCM Send	2-85
1012 – PCM Receive Warn.....	2-86
1013 – PCM Send AM Warn.....	2-86
1014 – PCMM Fail Send Message Error	2-87
1015 – PCMM Success Send Message.....	2-87
1016 – PCMM Fail Over RKS	2-88
1017 – PCMM Fail Too Busy	2-89
1020 – PCM Reject No PEP.....	2-89
1021 – PCMM Reject Invalid Gate.....	2-90
1022 – PCMM Reject AMID Mismatch.....	2-91
1023 – PCMM Reject SubId Mismatch	2-91
1024 – PCMM Reject Unknown Subscriber	2-92
1025 – PCMM Reject Unauth AMID.....	2-93
1026 – PCMM Reject Unknown Service	2-94
1027 – PCMM Reject Incompat Envelop	2-94
1028 – PCMM Reject Exceed CMTS Limit	2-95
1029 – PCMM Failed To Send Gate Message.....	2-96
1050 – Policy Reject2	2-97
1051 – Policy Reject	2-97
1101 – DQOS Downstream Connection Closed Clear Set.....	2-98
1102 – MSC Conn Lost Lost Clear.....	2-99
1104 – DQOS AM Connection Closed Clear Set.....	2-99
1110 – DQOS Received CMS	2-100
1111 – DQOS Sending.....	2-100
1112 – DQOS Received.....	2-101
1113 - DQOS Send CMS Warn	2-101

1120 - DQOS Reject No CMTS	2-102
1121 - DQOS Reject Gate	2-103
1123 - DQOS Reject Sub ID	2-103
1124 - DQOS Reject Subscriber	2-104
1129 - DQOS Reject.....	2-104
1150 - DQOS Policy Reject.....	2-105
1204 - SPC Conn Closed Closed Clear	2-106
1209 - SPC DQOS Gate Delete	2-106
1210 - SPC DQOS Received.....	2-107
1213 - SPC DQOS Send CMS Warn.....	2-107
1221 - SPC DQOS Global Session Reject	2-108
1231 - SPC DQOS Ingress Reject	2-109
1232 - SPC DQOS Gate Reject.....	2-109
1233 - SPC DQOS Gate Drop	2-110
1250 - SPC DQOS Policy Reject	2-110
1370 - BRAS IP Declared Static.....	2-111
1401 - Diam Conn Opened W Peer	2-112
1402 - Connectivity Lost Lost Clear	2-112
1403 - Connectivity Degraded Degraded Clear	2-113
1404 - Send Message Debug Info	2-113
1405 - Receive Message Debug Info	2-114
1406 - Receive Message EXC	2-115
1407 - Peer Status Change Notice Warn	2-115
1408 - New Conn Rejected New Conn Rejected Clear.....	2-116
1409 - Reject Missing AVP	2-116
1410 - Message Timeout.....	2-117
1411 - Duplicate Message.....	2-118
1412 - Send Response Info Warn Debug.....	2-118
1413 - Receive Response Info Warn Debug	2-119
1414 - SCTP Path Status Changed Changed Clear	2-119
1415 - Diam CR Conn Opened W Peer.....	2-120
1416 - Diam CR Conn Disconnected W Peer	2-120
1417 - CR Message Forwarded	2-121
1420 - Diam Reject No PCEF Warn	2-122
1421 - Diam Missing Profile For Media	2-122
1440 - Diam No Associated NE.....	2-123
1441 - Rule Fail	2-124
1442 - Rule Retry	2-124
1443 - Retry Fail Error	2-125
1444 - Rule Retry Canceled.....	2-125
1445 - Rule Retry Error Too Many	2-126
1446 - Max PDN Connections	2-127
1447 - Diam Too Many Sessions.....	2-127

1450 – SCE GX No Profile.....	2-128
1470 – Diam Session Cleanup Start.....	2-128
1471 – Diam Session Cleanup Send RARs	2-129
1472 – Diam Session Cleanup Complete.....	2-130
1473 – PCMM Session Cleanup Send GateInfos	2-130
1474 – PCMM Session Cleanup Start.....	2-131
1475 – PCMM Session Cleanup Complete.....	2-131
1476 – Diam Session Cleanup Built Complete	2-132
1477 – PCMM Session Cleanup Built Complete	2-132
1600 – DBPLUGIN No Match Warn	2-133
1601 – LDAP Conn To.....	2-133
1602 – LDAP Closing Conn To	2-134
1605 – LDAP Conn Failed Failed Clear	2-135
1610 – LDAP Search Fail.....	2-135
1611 – LDAP Search	2-136
1612 – LDAP Search Results	2-136
1613 – LDAP Search No Matches.....	2-137
1614 – LDAP Multi Match.....	2-137
1615 – LDAP Search Fail2.....	2-138
1617 – LDAP Modify Entry	2-138
1619 – LDAP Modify Unexpected Error	2-139
1620 – LDAP Queue Distress.....	2-140
1621 – LDAP Queue Cleared	2-140
1622 – LDAP Queue Full	2-141
1623 – LDAP Modify Fail2.....	2-141
1624 – LDAP Modify Fail	2-142
1626 – No Configured Data Sources	2-142
1630 – DHCP Unexpected Event ID Set Clear	2-143
1631 – DHCP Unable To Bind Event ID	2-144
1632 – DHCP Response Timeout Event ID	2-144
1633 – Bad Relay Address Event ID Set Clear	2-145
1634 – Bad Primary Address Event ID Set Clear.....	2-145
1635 – Bad Secondary Address Event ID Set Clear.....	2-146
1641 – Searching Event ID.....	2-146
1642 – Results Event ID	2-147
1661 – EL Bad Realm.....	2-147
1662 – EL Bad Address	2-148
1663 – EL Searching.....	2-148
1664 – EL Search Results.....	2-149
1665 – EL No Matches.....	2-149
1666 – EL Unexpected Search Failure.....	2-150
1667 – EL Subscribing	2-151
1668 – EL Subscribe Results	2-151

1669 – EL Subscribe Fail	2-152
1670 – EL Unsubscribing	2-152
1671 – EL Unsubscribe Results	2-153
1672 – EL Unsubscribe Failure.....	2-153
1673 – EL Notification.....	2-154
1674 - EL Updating.....	2-154
1675 - EL Update Failure	2-155
1676 - EL Update Out of Sync.....	2-155
1681 – MSR Connection	2-156
1682 – MSR Connection Closing	2-156
1684 – SPR Connection Closed	2-157
1685 – MSR DB Not Reachable	2-158
1686 – MSR Search.....	2-158
1687 – MSR Search Result.....	2-159
1690 – MSR Search Fail	2-159
1691 – MSR Update	2-160
1692 – MSR Update Result	2-160
1693 – MSR Update Fail.....	2-161
1694 – MSR Sub.....	2-161
1695 – MSR Sub Result	2-162
1696 – MSR Sub Fail	2-162
1697 – MSR Unsub.....	2-163
1698 – MSR Unsub Result	2-164
1699 – MSR Unsub Fail	2-164
1711-BRAS Handle DRQ	2-165
1801 – PCMM No PCEF.....	2-165
1805 - PCMM No Connection PCEF.....	2-166
2198 – SMSR SMSC Switched to Primary	2-166
2199 - SMSR SMSC Switched to Secondary.....	2-167
2210 - Reached Max Gates Event ID Clear	2-167
2211 – Reached Max GPI Event ID Set Clear	2-168
2212 - Incrementing GPI Event ID	2-169
2213 – Decrementing GPI Event ID	2-169
2300 – Time Period Changed	2-170
2301 – Transition Started	2-170
2302 – Transition Aborted	2-171
2303 – Transition Succeeded	2-171
2304 – Transition Failed	2-172
2305 – Transition Aborted On Demand.....	2-173
2306 – Tasks Scheduled On Demand.....	2-173
2547 – SMS Delivery Date In Past	2-174
2548 – SMS Send Global Billing Day	2-174
2549 – SMSR Queue Full	2-175

2550 – SMS Not Enabled.....	2-175
2551 – SMS Config Endpoint	2-176
2552 – SMS Send Success.....	2-177
2553 – SMS Billing Day Send Failure.....	2-177
2554 – SMS Send Delivery Date	2-178
2555 – SMS Send Error.....	2-178
2556 – SMS Send Failure.....	2-179
2557 – SMS Failure No MSISDN	2-179
2558 – SMS Connection Established To SMSC	2-180
2559 – SMSR SMSC Conn Closed.....	2-181
2560 – Email Not Enabled Info Warn	2-181
2561 – Email Config Endpoint.....	2-182
2562 – Email Send Success	2-182
2563 – Email Send Error.....	2-183
2564 – Email Send Failure	2-183
2565 – SMSR SMTP Conn Closed.....	2-184
2566 – SMTP Connection Established Warn	2-184
2567 – SMTP Connection Error.....	2-185
2568 – HTTP Connection Established.....	2-186
2569 – HTTP Connection Error SMSR HTTP Conn Closed	2-186
2570 – HTTP Queue Clear Size Reached.....	2-187
2571 – Generic Notification Send Error.....	2-187
2611 – MSR Receive Notification.....	2-188
2700 – Binding Created	2-188
2701 – Binding Released	2-189
2702 – Binding Found	2-189
2703 - Binding Not Found	2-190
2704 - Binding Release Task	2-191
2705 – Duplicate Bindings	2-191
2706 – Suspect Cleanup Start.....	2-192
2707 – Suspect Cleanup Finished	2-192
2708 – DRA Cleanup Task Finished Iter.....	2-193
2710 – RADIUS Cleanup RADIUS Server Stop	2-193
2711 – RADIUS Cleanup Failed.....	2-194
2712 – RADIUS Cleanup Started.....	2-195
2713 – RADIUS Rejected On TDF Failure RADIUS Send Failure.....	2-195
2720 – Mapping Cleanup Start	2-196
2721 – Mapping Cleanup Finished	2-196
2900 – ADMISSION Protocol Busy Event.....	2-197
2901 – ADMISSION Protocol Clear Event	2-197
2902 – ADMISSION Component Busy Event.....	2-198
2903 – ADMISSION Component Clear Event.....	2-199
2904 – Diameter Too Busy Set Clear.....	2-199

2905 – RADIUS Too Busy Clear	2-200
3000 – Trace Log Rate Limit	2-200
3100 – Cert Interval Days	2-201
3101 – Cert Interval	2-202
4000 – Policy Critical Alarm Clear.....	2-202
4001 – Policy Major Alarm Clear	2-203
4002 – Policy Minor Alarm Clear.....	2-203
4048 – PCMM Unknown GateID.....	2-204
4063 – NAC Session Context Format Error	2-204
4069 – CAC Remove Fail	2-205
4080 – NAC Session Lookup Fail	2-206
4143 – CAC DB Write Fail	2-206
4154 – NAC VOD Server Activate	2-207
4155 – NAC VOD Server Deactivate	2-207
4156 – PCMM Unknown	2-208
4157 – PCMM Protocol Error	2-208
4208 – CAC Dupe Session Status	2-209
4300 - RC Conn Lost.....	2-209
4301 - RC Conn Restore	2-210
4302 – RC Unreachable	2-210
4303 – RC Log Download Fail	2-211
4550 – Policy Info.....	2-211
4551 – Policy Warn	2-212
4552 – Policy Debug	2-213
4560 – Policy Trace Action Emergency.....	2-213
4561 – Policy Trace Action Alert.....	2-214
4562 – Policy Trace Action Critical.....	2-214
4563 – Policy Trace Action Error	2-215
4564 – Policy Trace Action Warning	2-215
4565 – Policy Trace Action Notice.....	2-216
4566 – Policy Trace Action Info.....	2-216
4567 – Policy Trace Action Debug.....	2-217
4600 – Secondary Connection Rejected	2-217
4601 – Secondary Connection Reverted.....	2-218
4610 – SH Connection OPT	2-219
4700 – UME CMD Return Msg.....	2-219
4701 – Diam Msg Send Failed.....	2-220
6000 – Sync Log Wireline Subact Log.....	2-220
6001 – Subact Log Wireline Sync Log.....	2-221
6102 – State Sync Mgr Endpoint.....	2-222
6103 – VOD Terminate CAC Session	2-222
6105 – PCMM XML Syntax Error	2-223
6200 – NAC Abnormal Session Delete	2-223

6201 – NAC Normal Session Delete	2-224
6202 – NAC Allow Session.....	2-225
6203 – NAC Reject No Path.....	2-225
6204 – NAC Reject Sub	2-226
6205 – NAC Allow Sub	2-227
6206 – NAC Missing Sub Account	2-227
6207 – NAC Unknown Sub	2-228
6208 – NAC Policy Reject	2-229
6209 – NAC Static Dynamic Defn	2-230
6210 – NAC Reject No Endpoint	2-230
6211 – IP Already Static	2-231
6400 – BRAS Extension	2-231
6401 – BRAS Contraction.....	2-232
6402 – BRAS Overflow.....	2-233
6403 – COPS Connection Accepted	2-233
6404 – BRAS Connection Closed Clear	2-234
6405 – COPS Unknown Gateway Clear	2-235
6406 – BRAS Conn Closed.....	2-235
6407 – BRAS Handle OPN.....	2-236
6408 – BRAS Send Dec Debug	2-237
6409 – BRAS Send SSQ	2-237
6410 – BRAS State Sync Complete	2-238
6411 – BRAS Endpoint	2-238
6412 – BRAS Handle DRQ Msg.....	2-239
6413 – NAC Stale BRAS Endpoint	2-240
6414 – BRAS Send DEC	2-240
6415 – Update Session.....	2-241
6416 – Handle Delete	2-241
6417 – Handle Ack.....	2-242
6418 – State Sync Mgr Sync Start.....	2-243
6419 – State Sync Mgr Gateway	2-243
6420 – State Sync Mgr Cold Reboot	2-244
6421 – Handle Delete Subscriber.....	2-245
6422 – State Sync Mgr Delete Stale	2-245
6423 – State Sync Mgr Warn Reboot	2-246
6424 – State Sync Mgr AYT	2-247
6425 – State Sync Mgr AWD	2-247
6426 – BRAS Drop	2-248
6427 – BRAS Scrubber Logout.....	2-249
7001 – CAC Session Create Error	2-249
7002 – CAC Sync Session Recreate.....	2-250
7003 – CAC Session Recreate Fail	2-250
7010 – CAC Session ID List Read Error.....	2-251

7011 – CAC Session Create Fail	2-252
7013 – CAC Sync Error2	2-252
7014 – CAC Remove Session Failed.....	2-253
7015 – CAC Resource Release Fail	2-253
7019 – CAC Session Create.....	2-254
7023 – NAC VOD Server Sync.....	2-255
7025 – NAC Handle Error	2-255
7027 – NAC Send Error Reply	2-256
7031 – Exception Writing Session.....	2-256
7032 – CAC Resource Error.....	2-257
7034 – CAC Session Remove Sync Mismatch.....	2-258
7035 – CAC Session Remove Sync Timeout	2-258
7036 – CAC Sync Mismatch Session Removal	2-259
7038 – NAC VOD Synchronizer Activate	2-259
7039 – NAC VOD Synchronizer Deactivate	2-260
7047 – CAC Sync Start	2-261
7048 – CAC Sync End	2-261
7052 – CAC Resource Reserve Fail.....	2-262
7054 – CAC Dupe Session	2-263
7055 – CAC Session Missing	2-263
7056 – CAC Session Missing Remove	2-264
7057 – CAC Keep Alive Request	2-264
7058 – CAC Session List Status.....	2-265
7059 – CAC Session Detail Status.....	2-266
7060 – CAC Version Status Report.....	2-266
7061 – CAC Reserve Session Status	2-267
7062 – CAC Session Release Status	2-267
7063 – CAC Keep Alive No Response	2-268
7064 – CAC Session Release Error	2-269
7065 – CAC Session Release.....	2-269
7066 – CAC Version Status	2-270
7067 – CAC Version Report.....	2-270
7068 – CAC Invalid Version Report	2-271
7069 – CAC Keep Alive Send.....	2-272
7070 – CAC Keep Alive Response.....	2-272
7071 – CAC Sync Mismatch	2-273
7072 – CAC Sync Mismatch VOD.....	2-273
7073 – Invalid Bit Rate	2-274
7075 – CAC Session Create VOD Fail.....	2-275
7076 – CAC Sync Error	2-275
7078 – CAC Session List Error	2-276
7079 – VOD Sync Now.....	2-277
7080 – CAC Sync Start Server	2-277

7081 – CAC Sync Status	2-278
7082 – CAC Max Sync Fail	2-279
7083 – CAC Dupe Session Status Info	2-279
7084 – CAC Sync VOD Session	2-280
7085 - CAC Sync Session	2-281
8001 – BoD Initial Event Log.....	2-281
8020 – BoD Missing Params HTTP	2-282
8021 – BoD Failure HTTP	2-282
8022 – BoD Unknown SVC Name HTTP	2-283
8023 – BoD Expected Params HTTP	2-283
8024 - BoD Classifier Already Active HTTP	2-284
8025 - BoD Classifier Not Active HTTP	2-285
8050 - BoD Success HTTP	2-285
8070 – BoD Failure SOAP	2-286
8080 - BoD Success SOAP	2-286
8100 - BoD Establish Connection PS.....	2-287
8102 – BOD Retry Connection PS.....	2-287
8103 - BOD Drop Connection PS.....	2-288
8104 - BoD Disconnect Connection PS	2-289
8105 - BoD Disconnect Connection Failure PS	2-289
8106 - BoD Establish Connection Failure PS.....	2-290
8200 - BoD Change Event Log Level	2-290
8250 – BoD Start Session Cleanup Task.....	2-291
8251 – BoD Complete Session Cleanup Task.....	2-292
8252 – BoD Database Backup Failed.....	2-292
8253 – BoD Start Database Backup	2-293
8254 – BoD Finish Database Backup.....	2-293
8260 – BoD Cluster Reinitialized	2-294
8300 – BoD Send Message Debug.....	2-294
8301 – BoD Receive Message Debug Warning	2-295
8302 – BoD Request Timeout	2-295
8310 – BoD PCMM Incorrect Service XML Syntax	2-296
8311 – BoD PCMM Miss Required Fields	2-297
8312 – BoD Diameter Incorrect Service XML Syntax	2-297
8313 – BoD Duplicate Service	2-298
8314 – BoD Service Multiple Used	2-298
8315 – BoD Active Session Existed.....	2-299
8320 – BoD PCMM Create Session Failed.....	2-299
8321 – BoD PCMM Delete Session Failed	2-300
8400 – BoD MAC Translation Failed Due to Session ID Connection Failed	2-300
8401 – BoD MAC Translation Succeeded.....	2-301
8402 – BoD MAC Translation Failed Due To No IP Address For Session ID	2-301
8403 – BoD MAC Translation Failed Due To Response Failed For Session ID.....	2-302

8404 – BoD MAC Translation Failed Due To Incorrect MAC Translation URL for Session ID.....	2-303
8405 – BoD MAC Translation Failed Due To MAC Address Connection Failure.....	2-303
8406 – BoD MAC Translation Failed Due To No IP Address For MAC Address	2-304
8407 – BoD MAC Translation Failed Due To Response Failed For MAC Address.....	2-304
8408 – BoD MAC Translation Failed Due To Incorrect MAC Translation URL For MAC Address	2-305
8410 – BoD MAC Translation Failed Due to Configuration Error	2-305
8411 – BoD Session Notification Return Success.....	2-306
8412 – BoD Session Notification Return Other Status.....	2-306
8413 – BoD Session Notification Expire	2-307
8414 – BoD Session Notification Retry	2-308
8420 – IPv6 Subnets Filtering Stats	2-308
8421 – IPv6 Subnets Filtering Stats All	2-309
8422 - IPv6 Subnets Aggregation Stats	2-309
8423 - IPv6 Subnets Aggregation Stats All.....	2-310
8424 – IPv6 Subnets Setting To MA Success	2-310
8425 – IPv6 Subnet Setting To MA Failure.....	2-311
8426 – Subnets Overlapped Details.....	2-311
8427 – Subnet Overlap Detect Task Start.....	2-312
8428 – Subnet Overlap Detect Task End.....	2-313
8429 – IPv4 Subnets Filtering Stats All	2-313
8430 – IPv4 Subnets Filtering Stats	2-314
8431 – OSSI Triggered CMTS Rediscovery	2-314
8432 – Subnets Overlapped CMTS Details	2-315
8500 – MA Server Start	2-316
8501 – BoD HTTP Request Fail.....	2-316
8502 – BoD Classifier Active SubIP.....	2-317
8503 – BoD PS Conn Drop.....	2-317
8504 – BoD Disconn.....	2-318
8505 – BoD Disconn Fail	2-319
8506 – BoD Conn Fail	2-319
8507 – BoD DB Auto Delete Start	2-320
8508 – BoD DB Auto Delete End	2-320
8509 – BoD Send Debug.....	2-321
8510 – BoD Received Info	2-321
8511 – BoD Received Warn.....	2-322
8512 – BoD MAC Translate Success	2-323
8513 – BoD MAC Translate IP Fail	2-323
8514 – BoD MAC Translate Parse Fail	2-324
8515 – BoD MAC Translate MAC Fail	2-324
8516 – BoD MAC Translate Conn MAC Fail	2-325
8517 – BoD MAC Translate IP MAC Fail	2-325

8518 – BoD MAC Translate Parse MAC Fail	2-326
8519 – BoD MAC Translate Incorrect MAC Fail	2-327
8520 – Bod Service Parse Fail	2-327
8521 – BoD Socket Closed	2-328
8522 – BoD RDR Start Error	2-328
8523 – BoD RDR Port Busy	2-329
8524 – BoD RDR Fatal Error	2-329
8525 – BoD Start MSG Processing Debug	2-330
8526 – BoD Stop MSG Processing	2-330
8527 – BoD Start MSG Processing Info	2-331
8528 – Edge OAM Device Discovered.....	2-331
8529 – PCMM Send AM Info	2-332
8530 – PCMM Receive	2-333
8531 – DQOS Send CMS Info.....	2-333
8532 – SPC DQOS Send CMS Info	2-334
8534 – BoD RDR Quota MSG Processing Debug.....	2-335
8535 – BoD RDR Quota MSG Processing Info.....	2-335
8540 – BoD Received Debug	2-336
8541 – BoD Start Msg Processing Warn.....	2-336
8600 – BoD Invalid Session ID Arg	2-337
8601 – BoD PCMM Request Reject.....	2-337
8602 – BoD PCMM Mode Not Enabled.....	2-338
8603 – BoD Diameter Mode Not Enabled	2-339
8700 – BoD Admission Protocol Busy Event	2-339
8701 – BoD Admission Protocol Clear Event	2-340
8702 – BoD Admission Component Busy Event.....	2-340
8703 – BoD Admission Component Clear Event	2-341
8704 – BoD PCMM Too Busy Set Clear.....	2-341
10000 – ADS Connection Established	2-342
10001 - ADS Connection Closed.....	2-343
10002 - ADS Connection Lost Set Lost Clear	2-343
10003 – ADS Receive Error.....	2-344
10004 – ADS Send Error.....	2-344
10005 – ADS Error	2-345
10006 – Sy Receive Notification.....	2-345
10007 – Sy Bad Realm	2-346
10008 – Sy Bad Address	2-346
10009 – Sy Search.....	2-347
10010 – SY Search Results.....	2-348
10012 – Sy Search Error.....	2-348
10013 – Bad XML from SPR	2-349
10014 – TDF Connection Closed.....	2-349
10015 – Exceeds Max Allowed AVP Conditional Policy Info AVP	2-350

10020 – CMP Started	2-350
10021 – Import XML Add.....	2-351
10022 – Import XML Update	2-351
10023 – Import XML Delete	2-352
10024 – Import XML Fail	2-353
10025 – XML Add Fail	2-353
10026 – RC proxy apply2.....	2-354
10027 – RC proxy apply.....	2-354
10028 – RC proxy send.....	2-355
10029 – Stat Rsync Clean Task Start	2-355
10031 – Diam Service Invalid XML File	2-356
10032 – Stats Sync Task Start.....	2-356
10033 – Stats Sync Task Repository Success	2-357
10036 – Retry fail.....	2-357
10037 – DBPLUGIN No Match Debug	2-358
10038 – Email Not Enabled Info	2-359
10039 – RADIUS Server Init	2-359
10040 – RADIUS Server Start Notice	2-360
10041 – RADIUS Drop Invalid Warn	2-360
10042 – RADIUS Drop Bad MD5 Warn	2-361
10043 – RADIUS Sent	2-361
10044 – Policy Info Event.....	2-362
10045 – RADIUS Server Start Fail	2-362
10046 – RADIUS Received	2-363
10048 – SCTP Path Status	2-363
10100 – Avg Sess Size Exceeds Projected Set	2-364
10101 – Avg Sess Size Exceeds Projected Clear	2-364
10102 – Sess Size Reached Threshold Set.....	2-365
10103 – Sess Size Reached Threshold Clear	2-365
10104 – Avg Bind Size Exceeds Projected Set	2-366
10105 – Avg Bind Size Exceeds Projected Clear	2-367
10106 – Bind Size Reached Threshold Set	2-367
10107 – Bind Size Reached Threshold Clear.....	2-368
10108 – ReplicationStats Task Start	2-368
10109 – ReplicationStats Task Failed.....	2-369
10110 – ReplicationStats Task Success	2-369
10111 – ReplicationStats Task Finish.....	2-370
10112 – ReplicationStats Task Data Available.....	2-370
10113 – Sy On Demand Policy Action Failure.....	2-371
10114 – Diam Session Cleanup Results	2-371
10115 – Diameter Invalid Ancids Warning	2-372
10116 – PCEF Report Timeout	2-373
10117 – Subtrace Disabled Busy State.....	2-373

10118 – Subtrace Enabled Normal State	2-374
10119 – X1 Connection Lost	2-374
10120 – Duplicate Default Bearer Rule	2-375
10121 – Invalid Traffic Profile	2-375
10122 – X2 Connection Lost	2-376
10123 – Policy Logging Overflow	2-376
10124 – Subtrace Policy Logging Overflow	2-377
10125 – AN GW Failed.....	2-377
10126 – Max Wait Time Exceeded	2-378
10127 – Diameter Newer Session Detected.....	2-378
10128 – SY Reconciliation Status	2-379
10129 – Sy Reconciliation Stats	2-380
10130 – Unauthorized Non Emergency Session	2-380
10131 – PCEF Initiated Emergency Request.....	2-381
10132 – Sy Reconciliation QP Notif.....	2-381
10133 – SYNC MRA Session Binding	2-382
10135 - High Bandwidth Attempt.....	2-382
10140 – Diameter App Not Found Message.....	2-383
10141 – Diameter Peer Config Fail.....	2-384
10160 – Diam Invalid App Detect Info Warning.....	2-384
10200 – VNF server create	2-385
10201 – VNF server update	2-385
10202 – VNF server delete.....	2-386
10203 – VNFMGR get.....	2-386
10204 – VNFMGR get error.....	2-387
10205 – VNF operation error set.....	2-387
10206 – VNF operation error clear	2-388
10207 – VNF rest operation	2-388
10208 – VNF API unsupported version	2-389
10209 – VNF Operation Error	2-389
10210 – POI Incoming Request.....	2-390
10211 – POI Outgoing Request to PPI	2-391
10212 – POI Return Response to POA.....	2-391
10213 – POI Operation Error.....	2-392
10214 – Rest Response.....	2-392
10215 – POI Operation Error.....	2-393
11001 – Remote Diversion Set Clear.....	2-393
15000 – SCMP Sync Trace Succ.....	2-394
15010 – SCMP Init Succ.....	2-394
15101 – Mediation SPR Connection Exception	2-395
15102 – Mediation SPR Connection Timeout	2-395
15103 – Mediation SOAP Parameter Error	2-396
15104 – Mediation Open COMCOL Error	2-396

15105 – Mediation Operate COMCOL Error	2-397
15106 – Mediation SOAP Result Error	2-398
15107 – Mediation SPR Connection Request	2-398
15108 – Mediation SPR Connection Response	2-399
15109 – Mediation SOAP Request	2-399
15110 – SPR Connection Failed	2-400
15111 – SPR Connection Failed Clear	2-400
15112 – SPR License Limit Set	2-401
15113 – SPR License Limit Clear	2-401
15114 – SPR Timeout Error	2-402
15115 – Mediation Admission Protocol Busy Event	2-402
15116 – Mediation Admission Protocol Clear Event	2-403
15117 – Mediation Admission Component Busy Event	2-403
15118 – Mediation Admission Component Clear Event	2-404
15119 – Mediation SOAP Too Busy Set Clear	2-404
15120 – Mediation SOAP Response	2-405
15121 – Sync Server Error	2-405
15122 – Sync Stop Server Error	2-406
15123 – Sync Thread Uncaught Exception	2-406
15124 – Sync Exec CMD Fail	2-407
15125 – Sync Exec CMD Error	2-408
15126 - Sync Accept App Sync Request	2-408
15127 - Sync Reject App Sync Request	2-409
15128 - Sync App Sync Request Exception	2-409
15129 - Sync App Sync Response	2-410
15130 - Sync App Sync Response Exception	2-410
15131 - Sync TooBusy Reject Request	2-411
15132 - Sync Invalid Request	2-411
15133 - Sync Handle Request Exception	2-412
15134 - Sync Accept Sync Request	2-412
15135 - Sync Open COMCOL Fail	2-413
15136 - Sync Close COMCOL Fail	2-413
15137 – Sync Verify Success	2-414
15138 - Sync Verify Fail	2-414
15139 – Sync Resolve Success	2-415
15140 - Sync Resolve Fail	2-416
15141 – Sync Create DATS Success	2-416
15142 - Sync Create DATS Fail	2-417
15143 - Do Sync Fail	2-417
15144 - Sync Create Sync Response	2-418
15145 – Sync Handle Response Exception	2-418
15146 - Sync Disk Quota Exceed	2-419
15147 – Sync Disk No Space	2-419

15148 – Sync Disk No Space Clear	2-420
15149 – MRA Sig Device Filter Changed	2-420
15150 –Reject Non-Authorized Connection	2-421
15151 – Accept Authorized Connection.....	2-421
15152 – Retransmit Message	2-422
15153 – MPE Sig Device Filter Changed	2-422
15160 – Batch Operation Error	2-423
15161 – Batch Request Validation.....	2-423
15162 – Batch Handle Result	2-424
15163 – Batch Disk Quota Exceed	2-425
15164 – Batch Disk No Space	2-425
15165 – Batch Clean Up	2-426
15166 – Scheduled Task RAR Sent	2-426
15167 – Rebuild Diameter Peers.....	2-427
15200 – PM Gen Stats Sync Task Start	2-427
15201 – PM Gen Stats Sync Task Success	2-428
15202 – PM Gen Stats Sync Task Fail.....	2-428
15203 – PM Gen Stats Sync Task End	2-429
15204 – PM Stats Sync Task Start.....	2-429
15205 – PM Stats Sync Task Success	2-430
15206 – PM Stats Sync Task Fail	2-430
15207 – PM Stats Sync Task End.....	2-431
15208 – PM Stats Sync Task Repository Success	2-431
15209 – PM Stats Sync Task Repository Fail.....	2-432
15301 – SMS Stats Sync Task Start.....	2-432
15302 – SMS Stats Sync Task Success.....	2-433
15303 – SMS Stats Sync Task Fail.....	2-434
15304 – SMS Status Sync Task End	2-434
15305 – SMS Stats Sync Task Repository Success	2-435
15306 – SMS Stats Sync Task Repository Fail	2-435
17000 – Quota usage daily reset complete	2-436
17001 – Quota usage daily reset task start	2-436
17002 – Quota usage daily reset task is ready to send RARs.	2-437
17100 – MDF Soap Result Error.....	2-437
17102 – MDF Soap Parameter Error.....	2-437
17103 – MDF No QP Name Error.....	2-438
17104 – MDF Soap Illegal OPMD Change	2-438
17105 – MDF Soap Client Result Error	2-439
17106 – MDF Cannot Parse SDM Response	2-439
17107 – MDF IMSI Not In Range.....	2-440
17108 – MDF Soap Client Request	2-441
17109 - MDF Soap Client Response	2-441
17110 – MDF SPR Message.....	2-442

17111 – MDF Get Subscriber	2-442
17112 – MDF Illegal Notify Subscriber	2-443
17113 – MDF Soap Request	2-443
17114 – MDF Soap Response.....	2-444
17115 – MDF Out SPR Message.....	2-444
17116 – MDF IMSI Not In SPR.....	2-445
17118 – MDF IMSI In SPR.....	2-445
17119 – MDF IMSI In S-SPR	2-446
17120 – MDF DYQ Was Expired.....	2-446
17121 – MDF Quota Was Expired	2-447
17122 – MDF Deduct Usage Fail	2-447
17123 – MDF Deductible Quotas	2-448
17124 – MDF Reset For Deduct	2-448
17125 – MDF Do Deduct Usage.....	2-449
17301 – Clearance Started.....	2-449
17302 – Clearance Duplicating	2-450
17303 – Clearance Abort	2-450
17304 – Clearance Session Terminate	2-451
17305 – Clearance Finished	2-452
17306 – KT Reject Invalid Sub.....	2-452
17307 – PUA Failure of Reset.....	2-453

3 Alarms and Events

Alarms formatting information	3-1
Alarm and event types	3-2
Alarm and Event Severity Levels	3-3
Platform (31000-32800).....	3-4
31000 - S/W fault.....	3-4
31001 - S/W status.....	3-4
31002 - Process watchdog failure	3-5
31003 - Tab thread watchdog failure.....	3-5
31004 - Test Status.....	3-6
31005 - Test Fault	3-6
31100 - Database replication fault	3-6
31101 - Database replication to slave failure.....	3-7
31102 - Database replication from master failure.....	3-8
31103 - DB Replication update fault	3-9
31104 - DB Replication latency over threshold.....	3-9
31105 - Database merge fault	3-10
31106 - Database merge to parent failure	3-11
31107 - Database merge from child failure.....	3-11
31108 - Database merge latency over threshold	3-12
31109 - Topology config error	3-12

31110 - Database audit fault	3-13
31111 - Database merge audit in progress	3-14
31112 - DB replication update log transfer timed out.....	3-14
31113 - DB replication manually disabled.....	3-15
31114 - DB replication over SOAP has failed.....	3-15
31115 - Database service fault	3-16
31116 - Excessive shared memory	3-16
31117 - Low disk free.....	3-17
31118 - Database disk store fault	3-17
31119 - Database updatelog overrun.....	3-18
31120 - Database updatelog write fault	3-19
31121 - Low disk free early warning.....	3-19
31122 - Excessive shared memory early warning	3-20
31123 - Database replication audit command complete	3-20
31124 - ADIC error.....	3-21
31125 - Database durability degraded	3-21
31126 - Audit blocked	3-22
31127 - DB Replication Audit Complete	3-22
31128 - ADIC Found Error.....	3-23
31129 - ADIC Found Minor Issue.....	3-23
31130 - Network health warning.....	3-24
31131 - DB Ousted Throttle Behind.....	3-25
31132 - DB Replication Precedence Relaxed	3-25
31133 - DB Replication Switchover Exceeds Threshold.....	3-26
31134 - DB Site Replication To Slave Failure.....	3-26
31135 - DB Site Replication From Master Failure.....	3-27
31136 - DB Site Replication Precedence Relaxed.....	3-27
31137 - DB Site Replication Latency Over Threshold.....	3-28
31140 - Database perl fault	3-28
31145 - Database SQL fault.....	3-29
31146 - DB mastership fault	3-30
31147 - DB upsynclog overrun.....	3-30
31148 - DB lock error detected	3-31
31200 - Process management fault	3-31
31201 - Process not running	3-32
31202 - Unkillable zombie process.....	3-32
31206 - Process mgmt monitoring fault.....	3-33
31207 - Process resource monitoring fault	3-34
31208 - IP port server fault	3-34
31209 - Hostname lookup failed.....	3-35
31213 - Process scheduler fault.....	3-35
31214 - Scheduled process fault.....	3-36
31215 - Process resources exceeded	3-36

31216 - SysMetric configuration error	3-37
31217 - Network Health Warning	3-38
31220 - HA configuration monitor fault.....	3-38
31221 - HA alarm monitor fault	3-39
31222 - HA not configured	3-39
31223 - HA Heartbeat transmit failure	3-40
31224 - HA configuration error	3-40
31225 - HA service start failure	3-41
31226 - HA availability status degraded	3-41
31227 - HA availability status failed.....	3-42
31228 - HA standby offline.....	3-42
31229 - HA score changed	3-43
31230 - Recent alarm processing fault	3-44
31231 - Platform alarm agent fault.....	3-44
31232 - Late heartbeat warning	3-45
31233 - HA Path Down	3-45
31234 - Untrusted Time Upon Initialization	3-46
31235 - Untrusted Time After Initialization	3-47
31236 - HA Link Down	3-47
31240 - Measurements collection fault	3-48
31250 - RE port mapping fault.....	3-48
31260 - SNMP Agent	3-49
31261 - SNMP Configuration Error.....	3-49
31270 - Logging output.....	3-50
31280 - HA Active to Standby transition	3-51
31281 - HA Standby to Active transition	3-51
31282 - HA Management Fault.....	3-52
31283 - Lost Communication with server	3-52
31284 - HA Remote Subscriber Heartbeat Warning	3-53
31285 - HA Node Join Recovery Entry	3-53
31286 - HA Node Join Recovery Plan.....	3-54
31287 - HA Node Join Recovery Complete	3-54
31288 - HA Site Configuration Error	3-55
31290 - HA Process Status	3-55
31291 - HA Election Status	3-56
31292 - HA Policy Status	3-56
31293 - HA Resource Link Status	3-57
31294 - HA Resource Status	3-58
31295 - HA Action Status	3-58
31296 - HA Monitor Status.....	3-59
31297 - HA Resource Agent Info	3-59
31298 - HA Resource Agent Detail.....	3-60
31299 - HA Notification Status	3-60

31300 - HA Control Status.....	3-61
31301 - HA Topology Events.....	3-61
31322 - HA Configuration Error.....	3-62
32100 - Breaker Panel Feed Unavailable	3-62
32101 - Breaker Panel Breaker Failure.....	3-63
32102 - Breaker Panel Monitoring Failure.....	3-63
32103 - Power Feed Unavailable	3-63
32104 - Power Supply 1 Failure	3-64
32105 - Power Supply 2 Failure	3-64
32106 - Power Supply 3 Failure	3-65
32107 - Raid Feed Unavailable	3-65
32108 - Raid Power 1 Failure	3-66
32109 - Raid Power 2 Failure	3-66
32110 - Raid Power 3 Failure.....	3-67
32111 - Device Failure	3-67
32112 - Device Interface Failure.....	3-68
32113 - Uncorrectable ECC memory error	3-68
32114 - SNMP get failure	3-69
32115 - TPD NTP Daemon Not Synchronized Failure	3-69
32116 - TPD Server's Time Has Gone Backwards	3-71
32117 - TPD NTP Offset Check Failure.....	3-72
32300 - Server fan failure	3-74
32301 - Server internal disk error	3-74
32302 - Server RAID disk error.....	3-75
32303 - Server Platform error.....	3-75
32304 - Server file system error.....	3-76
32305 - Server Platform process error.....	3-77
32306 - Server RAM shortage error.....	3-78
32307 - Server swap space shortage failure	3-78
32308 - Server provisioning network error	3-79
32309 - Eagle Network A Error.....	3-80
32310 - Eagle Network B Error	3-80
32311 - Sync Network Error	3-81
32312 - Server disk space shortage error.....	3-81
32313 - Server default route network error.....	3-82
32314 - Server temperature error.....	3-83
32315 - Server mainboard voltage error	3-84
32316 - Server power feed error	3-85
32317 - Server disk health test error.....	3-86
32318 - Server disk unavailable error	3-87
32319 - Device error.....	3-88
32320 - Device interface error	3-88
32321 - Correctable ECC memory error	3-89

32322 - Power Supply A error.....	3-90
32323 - Power Supply B error	3-90
32324 - Breaker panel feed error	3-91
32325 - Breaker panel breaker error	3-92
32326 - Breaker panel monitoring error	3-95
32327 - Server HA Keepalive error	3-96
32328 - DRBD is unavailable.....	3-97
32329 - DRBD is not replicating.....	3-97
32330 - DRBD peer problem.....	3-98
32331 - HP disk problem	3-99
32332 - HP Smart Array controller problem.....	3-99
32333 - HP hpacucliStatus utility problem	3-100
32334 - Multipath device access link problem.....	3-101
32335 - Switch link down error.....	3-102
32336 - Half Open Socket Limit.....	3-102
32337 - Flash Program Failure	3-103
32338 - Serial Mezzanine Unseated	3-104
32339 - TPD Max Number Of Running Processes Error.....	3-104
32340 - TPD NTP Daemon Not Synchronized Error	3-105
32341 - TPD NTP Daemon Not Synchronized Error	3-106
32342 - NTP Offset Check Error	3-107
32343 - TPD RAID disk	3-108
32344 - TPD RAID controller problem	3-109
32345 - Server Upgrade snapshot(s) invalid.....	3-110
32346 - OEM hardware management service reports an error	3-110
32347 - The hwmgmtcliStatus daemon needs intervention	3-111
32348 - FIPS subsystem problem.....	3-112
32349 - File Tampering.....	3-112
32350 - Security Process Terminated.....	3-113
32500 - Server disk space shortage warning.....	3-113
32501 - Server application process error	3-114
32502 - Server hardware configuration error	3-115
32503 - Server RAM shortage warning	3-116
32504 - Software Configuration Error.....	3-116
32505 - Server swap space shortage warning.....	3-117
32506 - Server default router not defined	3-118
32507 - Server temperature warning	3-119
32508 - Server core file detected	3-120
32509 - Server NTP Daemon not synchronized	3-121
32510 - CMOS battery voltage low	3-122
32511 - Server disk self test warning.....	3-122
32512 - Device warning	3-123
32513 - Device interface warning	3-123

32514 - Server reboot watchdog initiated.....	3-124
32515 - Server HA failover inhibited	3-125
32516 - Server HA Active to Standby transition	3-125
32517 - Server HA Standby to Active transition	3-126
32518 - Platform Health Check failure	3-126
32519 - NTP Offset Check failure	3-127
32520 - NTP Stratum Check failure.....	3-128
32521 - SAS Presence Sensor Missing.....	3-129
32522 - SAS Drive Missing	3-130
32523 - DRBD failover busy	3-130
32524 - HP disk resync.....	3-131
32525 - Telco Fan Warning.....	3-132
32526 - Telco Temperature Warning.....	3-132
32527 - Telco Power Supply Warning	3-133
32528 - Invalid BIOS value	3-134
32529 - Server Kernel Dump File Detected.....	3-134
32530 - TPD Upgrade Failed	3-135
32531 - Half Open Socket Warning Limit.....	3-135
32532 - Server Upgrade Pending Accept/Reject	3-136
32533 - TPD Max Number Of Running Processes Warning.....	3-137
32534 - TPD NTP Source Is Bad Warning	3-137
32535 - TPD RAID disk resync	3-138
32536 - TPD Server Upgrade snapshot(s) warning	3-139
32537 - FIPS subsystem warning event	3-140
32538 - Platform Data Collection Error	3-140
32539 - Server Patch Pending Accept/Reject	3-141
32540 - CPU Power limit mismatch	3-141
32700 - Telco Switch Notification	3-142
32701 - HIDS Initialized.....	3-142
32702 - HIDS Baseline Deleted	3-143
32703 - HIDS Enabled	3-143
32704 - HIDS Disabled	3-143
32705 - HIDS Monitoring Suspended.....	3-144
32706 - HIDS Monitoring Resumed.....	3-144
32707 - HIDS Baseline Updated	3-144
QP (70000-70999).....	3-145
70001 – QP_procmgr failed	3-145
70002 – QP Critical process failed	3-146
70003 – QP Non-critical process failed	3-146
70004 – QP Processes down for maintenance.....	3-147
70007 - QP Resource Not Ready	3-147
70010 – QP Failed Server-backup Remote Archive Rsync.....	3-148
70011 – QP Failed System-backup Remote Archive Rsync	3-149

70012 – QP Failed To Create Server Backup	3-149
70013 – QP Failed To Create System Backup.....	3-150
70015 – Route Add Failed.....	3-150
70016 – No Available VIP Route	3-151
70017 – No Available Static IP	3-152
70020 – QP Master database is outdated.....	3-152
70021 – QP slave database is unconnected to the master	3-153
70022 – QP Slave database failed to synchronize	3-154
70023 – QP Slave database lagging the master	3-154
70024 - QP Slave database is prevented from synchronizing with the master.....	3-155
70025 – QP Slave database is a different version than the master.....	3-155
70026 – QP Server Symantec NetBackup Operation in Progress	3-156
70027 – QP Server Network Config Error.....	3-156
70028 – QP bonded interface is down	3-157
70029 – QP peer node bonded interface is down.....	3-158
70030 – QP backplane bonded interface is down	3-158
70031 – QP degrade because one or more interfaces are down.....	3-159
70032 – QP direct link does not work as configuration	3-159
70038 – QP has blocked IPv4 traffic on an OAM interface.....	3-160
70039 – QP has blocked IPv4 traffic on all interfaces	3-160
70040 – Failure to block IPv4 on the OAM interface	3-161
70041 – Failure to block IPv4 on the all interfaces	3-161
70042 – Failure to remove OAM IPv4 addresses from the cluster/site.....	3-162
70043 – Failure to remove all IPv4 addresses from the cluster/site.....	3-162
70044 – Failure to rollback changes for removing IPv4 addresses	3-163
70045 – DNS Server is not available	3-163
70050 – QP Timezone change detected	3-164
70500 – System Mixed Version	3-165
70501 – Cluster Mixed Version	3-165
70502 – Cluster Replication Inhibited.....	3-166
70503 – Server Forced Standby	3-167
70505 – ISO Mismatch.....	3-167
70506 – Upgrade Operation Failed	3-168
70507 – Upgrade In Progress	3-169
70508 – Server Is Zombie.....	3-169
Policy Server Alarms (71000-79999).....	3-170
71001 – Remote Diversion Not Possible.....	3-170
71002 – OM Stats Parse Error.....	3-170
71003 – OM Stats Exception Error.....	3-171
71004 – AM Conn Lost.....	3-172
71005 – OM Stats Value Exceed Error.....	3-172
71101 – DQOS Downstream Connection Closed	3-173
71102 – MSC Conn Lost	3-173

71103 – PCMM Conn Lost.....	3-174
71104 – DQOS AM Connection Closed	3-175
71204 – SPC Conn Closed.....	3-175
71402 – Connectivity Lost	3-176
71403 – Connectivity Degraded	3-176
71408 – Diameter New Conn Rejected	3-177
71414 – SCTP Path Status Changed	3-178
71605 – LDAP Conn Failed	3-178
71630 – DHCP Unexpected Event ID	3-179
71631 – DHCP Unable to Bind Event ID.....	3-179
71632 – DHCP Response Timeout Event ID.....	3-180
71633 – DHCP Bad Relay Address Event ID.....	3-180
71634 – DHCP Bad Primary Address Event ID	3-181
71635 – DHCP Bad Secondary Address Event ID	3-181
71684 – SPR Connection Closed	3-182
71685 – MSR DB Not Reachable	3-182
71702 – BRAS Connection Closed.....	3-183
71703 – COPS Unknown Gateway.....	3-184
71801 – PCMM No PCEF.....	3-184
71805 – PCMM Non Connection PCEF	3-185
72198 – SMSR SMSC Switched to Primary	3-185
72199 – SMSR SMSC Switched to Secondary	3-186
72210 – PCMM Reached Max Gates Event ID.....	3-186
72211 – PCMM Reached Max GPI Event ID.....	3-187
72501 – SCE Connection Lost.....	3-187
72549 – SMSR Queue Full	3-188
72559 – SMSR SMSC Connection Closed.....	3-189
72565 – SMSR SMTP Connection Closed.....	3-189
72575 – Policy Notification:Lost connection with destination URL.....	3-190
72703 – RADIUS Server Failed	3-190
72706 - RADIUS Server Corrupt Auth	3-191
72904 – Diameter Too Busy	3-191
72905 – Radius Too Busy	3-192
74000 – Policy Server Critical Alarm	3-192
74001 – Policy Server Major Alarm.....	3-193
74002 – Policy Server Minor Alarm	3-193
74020 – Stats Files Generator Delete Expire Files	3-194
74021 – Files Synchronization Failure	3-194
74022 - Files Uploading Failure	3-195
74102 - CMTS Subnet Overlapped.....	3-196
74103 - NES Without CMTS IP	3-196
74602 - Multiple Active In Cluster Failure.....	3-197
74603 - Max Primary Cluster Failure Threshold.....	3-198

74604 - MPE Cluster Offline Failure	3-198
74605 - Subscriber Trace Backup Failure	3-199
75000 - Policy Library Loading Failed	3-199
77904 - BOD PCMM Too Busy	3-200
77905 - BOD DIAMETER Too Busy	3-200
78000 - ADS Connection Lost	3-201
78001 - Rsync Failed	3-201
78850 - VNF operation error	3-202
79002 - Sess Size Reached Threshold	3-203
79003 - Avg Sess Size Exceed	3-203
79004 - Bind Size Reached Threshold	3-204
79005 - Avg Bind Size Exceed	3-205
79105 - Mediation SOAP Too Busy	3-205
79106 - SPR Connection Failed	3-206
79107 - Mediation Disk Quota Exceed	3-206
79108 - Mediation Disk No Space	3-207
79109 - SPR License Limit	3-207
79110 - Files Uploading Failure	3-208
79120 - Batch Disk Quota Exceeds	3-208
79995 - X1 Connection Lost	3-209
79996 - X2 Connection Lost	3-209
Policy Server Events (80000-89999)	3-210
80001 - DB State Transition	3-210
80002 - MySQL Relay Log Dropped	3-211
80003 - QP MySQL DB Level	3-211
82704 - Binding Release Task	3-212
84004 - Policy Info Event	3-212
86001 - Application Is Ready	3-213
86100 - CMP User Login	3-213
86101 - CMP User Login Failed	3-214
86102 - CMP User Logout	3-214
86200 - CMP User Promoted Server	3-215
86201 - CMP User Demoted Server	3-215
86300 - Sh Enable Failed	3-216
86301 - Sh Disable Failed	3-216
86303 - NW-CMP Apply Failed	3-217
86304 - S-CMP Unreachable	3-217
86305 - S-CMP Split Brain	3-218
86306 - CMP Apply Failed	3-218
86307 - S-CMP Sync Fails	3-219
86308 - NCMP Ref Obj Miss	3-219

Introduction

This chapter provides a content overview of this guide with a brief summary about incidents, notifications, and the ID ranges for alarms and events. It also includes contact information and how to locate product documentation on My Oracle Support.

About this Guide

The *Policy Management Troubleshooting Reference* compiles all available notifications, including any alarms or events generated by the system or a Policy action. Alarms alert an operator to action, while events provide information about an expected incident and can be used for debugging purposes. These notifications are sent from different areas of the Policy Management system and are stored for active viewing or historical purposes.

The *Policy Management Troubleshooting Reference* provides all available notifications that do not generate an alarm. Notifications use a 3-, 4-, or 5-digit ID, such as 401, 1683, or 10001.

Alarms and events are grouped under an ID range, which is associated with the type of alarm or event:

- [Platform \(31000-32800\)](#)
- [QP \(70000-70999\)](#)
- [Policy Server Alarms \(71000-79999\)](#)
- [Policy Server Events \(80000-89999\)](#)

How This Guide Is Organized

The information in this guide is presented in the following order:

- [Introduction](#)
- [Incidents, Notifications, and Logs Overview](#)
 - [About Incidents](#)
 - [About Notifications](#)
 - [About Logs](#)
- [Trace Log Notifications](#)
- [Alarms and Events](#)

- [Alarms formatting information](#)
- [Alarm and Event Severity Levels](#)
- [Platform \(31000-32800\)](#)
- [QP \(70000-70999\)](#)
- [Policy Server Alarms \(71000-79999\)](#)
- [Policy Server Events \(80000-89999\)](#)
- [#unique_21](#)

Scope and Audience

This guide is intended for trained and qualified system operators and administrators who are responsible for managing a Policy Management system.

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See [Locate Product Documentation on the Oracle Help Center Site](#) for more information on related product publications.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.

A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the PDF link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

<http://education.oracle.com/communication>

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

My Oracle Support

My Oracle Support is your initial point of contact for all product support and training needs. A representative at Customer Care Center can assist you with My Oracle Support registration.

Call the My Oracle Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
 - For Technical issues such as creating a new Service Request (SR), Select 1
 - For Non-technical issues such as registration or assistance with MOS, Select 2

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

List of Figures

3-1	Breaker Panel LEDs.....	3-93
3-2	Breaker Panel Setting.....	3-94

List of Tables

3-1	Alarm and Event Types.....	3-2
-----	----------------------------	-----

Incidents, Notifications, and Logs Overview

This chapter describes the concepts of incidents, notifications, and logs, and provides a procedure for configuring log settings.

About Incidents

There are two types of incidents:

System incident

An occurrence in the system, such as establishing a connection to a remote server. The system incident is further divided into platform-level and application-level incidents. Platform-level system incidents send alarms and events; application-level system incidents send trace log notifications, and in some cases, alarms and events.

Policy Action incident

Occurs when an operator uses policy actions to generate notifications based on policy execution. Policy action incidents can send trace log notifications, syslog notifications, and alarms and events.

The incident definition contains details about all notifications, such as trace log severity, message text, and alarm or event information.

Incidents can generate notifications. An example incident is trace event ID 1004 PCMM: Lost connection with AM {ID} which can generate an event in the trace log and an alarm as well as an SNMP trap. Some incidents can generate more than one type of notification. For example, a trace log notification and an alarm. The ID number indicates the source of the alarm or event as shown in the ID ranges below:

- [Platform \(31000-32800\)](#)
- [QP \(70000-70999\)](#)
- [Policy Server Alarms \(71000-79999\)](#)
- [Policy Server Events \(80000-89999\)](#)

About Notifications

A notification is a message sent by an incident. There are various logging mechanisms that receive these notifications, as well as an alarm system to notify operators of issues that may need action. Notifications may generate a trace log, syslog, and an alarm or event.

About Logs

Log files receive various types of notifications and log them for historical purposes.

There are several types of logs:

- Trace Log
- Policy Log
- Syslog
- SMS Log
- SMPP Log
- SMTP Log
- HTTP Log
- Session Synchronization Log

Refer to the *CMP User Guide* for information on viewing logs.

Viewing Policy Server Logs

The log files trace the activity of a Policy Management device. You can view and configure the logs for an individual cluster.

To view the log:

1. From the Policy Server section of the navigation pane, select **Configuration**.

The content tree displays a list of policy server groups.

2. From the content tree, select the Policy Management device.

The Policy Server Administration page opens in the work area.

3. Select the **Logs** tab.

Depending on your mode and release, you can configure the following logs:

- **Trace log**
Records application-level notifications.
- **Trace Log Forwarding**
Forwards cluster-level notifications.
- **Policy Log Settings**
Records the policy-level messages.
- **Policy Syslog Forwarding**
Records policy-processing activity. Supports the standard UNIX logging system, in conformance with RFC 3164.
- **SMS log**
Contains all Short Messaging Service messages sent by the MPE device as well as any ACK messages received from an SMS Center (SMSC) server or its equivalent.
- **SMPP log**

Contains all Short Message Peer-to-Peer Protocol (SMPP) notifications sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server.

- **SMTP log**

Contains all Simple Mail Transfer Protocol (SMTP) messages sent by the MPE device.

- **HTTP log**

Contains all Hypertext Transfer Protocol (HTTP) messages sent by the MPE device.

Viewing the Trace Log

The trace log records Policy Management application notifications, such as protocol messages, policy messages, and custom messages generated by policy actions, for individual servers. Trace logs are not replicated between servers in a cluster, but they persist after failovers. You can use the trace log to debug problems by tracing through application-level messages.

The activity of the Policy Rules Engine is recorded in a trace log at eight levels: Emergency (ID 4560), Alert (ID 4561), Critical (ID 4562), Error (ID 4563), Warning (ID 4564), Notice (ID 4565) Info (ID 4566), and Debug (ID 4567). You can configure the severity level of messages that are recorded in the trace log.

To view the Trace log:

1. Select the device to view:

- To view an MPE device, from the **Policy Server** section of the navigation pane, select **Configuration**.
- To view an MRA device, from the **MRA** section of the navigation pane, select **Configuration**.

The content tree displays a list of groups; the initial group is **ALL**.

2. From the content tree, select the device.

The appropriate Administration page opens in the work area.

3. On the Administration page, select the **Logs** tab.

Log information for the selected device is displayed.

4. Click **View Trace Log**.

While data is being retrieved, the in-progress message Scanning Trace Logs appears.

When the Trace Log Viewer window opens in a new browser window, all events contain the following information:

- **Date/Time**

Event timestamp. This time is relative to the server time.

- **Code**

The event code or ID number.

- **Severity**
Severity level of the event. Application-level trace log entries are not logged at a higher level than Error.
- **Message**
The message associated with the event. If additional information is available, the event entry shows as a link. Click the link to see additional detail in the frame below.

5. Filter the events displayed using the following:

- **Trace Log Viewer for Server**
Select the individual server within the cluster.
- **Start Date/Time**
Click  (calendar icon), select the starting date and time, then click **Enter**.
- **End Date/Time**
Click  (calendar icon), select the ending date and time, then click **Enter**.
- **Trace Codes**
Enter one or a comma-separated list of trace code IDs. Trace code IDs are integer strings up to 10 digits long.
- **Use timezone of remote server for Start Date/Time**
Select to use the time of a remote server (if it is in a different time zone) instead of the time of the CMP server.
- **Severity**
Filter by severity level. Events with the selected severity and higher are displayed. For example, if the severity selected is **Warning**, the trace log displays events with the severity level **Warning** and higher.
- **Contains**
Enter a text string to search for. For example, if you enter `connection`, all events containing the word `connection` display.

Note: The **Start Date/Time** setting overrides the **Contains** setting. For example, if you search for events happening this month, and search for a string in events last month and this month, only results from this month are listed.

6. After entering the filtering information, click **Search**.

The selected events are displayed. By default, the window displays 25 events per page.

7. To change the number of events per page, select a value from the **Display results per page** list.

You can change this to 50, 75, or 100 events per page.

Note: Events that occur after the Trace Log Viewer starts are not visible until you refresh the display.

8. To refresh the display, click any of the following:

- **Show Most Recent**

Applies filter settings and refreshes the display. This displays the most recent log entries that fit the filtering criteria.

- **Next/Prev**

When the number of trace log entries exceeds the page limit, pagination is applied. Use the **Prev** or **Next** buttons to navigate through the trace log entries. When the **Next** button is not visible, you have reached the most recent log entries; when the **Prev** button is not visible, you have reached the oldest log entries.

- **First/Last**

When the number of trace log entries exceeds the page limit, pagination is applied. Use the **First** and **Last** buttons to navigate to the beginning or end of the trace log. When the **Last** button is not visible, you have reached the end; when the **First** button is not visible, you have reached the beginning.

9. Click **Close**.

The trace log window closes.

Syslog Support

Notifications generated by policy actions are sent to the standard UNIX syslog. No other notifications are forwarded to the syslog. For information on policy actions, see the *Policy Wizard Reference*.

Note: These logs are separate from the TPD syslogs.

You can define multiple destinations for notifications and filter notifications by severity level. For more information, see [Configuring Log Settings for Servers in a Cluster](#).

The CMPP Log

The CMPP log contains all CMPP messages sent and received on the CMPP client, including state report if **Delivery Receipt** is enabled. This log records details about each message and tracks the success or failure of sending that message to a configured Short Message Service Center (SMSC). If messages are dropped by the short message relay (SMSR) application, then that action is logged so that all triggered messages can be tracked.

You can configure filter notifications by severity level. See [Configuring Log Settings for Servers in a Cluster](#) to modify the settings.

The SMS Log

The SMS log, `/var/Camiant/log/smsr.log`, contains all Short Message Service (SMS) messages sent by the MPE device as well as any ACK messages received from an SMS Center (SMSC) server or its equivalent. You can configure the severity level as well as the destination IP addresses of messages that are written to the SMS log. The default severity level is WARN. See [Configuring Log Settings for Servers in a Cluster](#) for more information.

The SMPP Log

The SMPP log is a policy action-generated notification that contains all Short Message Peer-to-Peer Protocol notifications sent by the MPE device as well as delivery receipts from a Short Message Service Center (SMSC) server. In SMPP or XML mode, SMPP information appears on the **Logs** tab of the Policy Server Administration page. You can modify the severity of messages that are written to the SMPP log on the MPE configuration page. The default severity is WARN. See [Configuring Log Settings for Servers in a Cluster](#) to modify the settings.

The SMTP Log

The SMTP log contains all Simple Mail Transfer Protocol (SMTP) messages sent by the MPE device, as well as any ACK messages received from a Mail Transfer Agent (MTA). In SMPP or XML mode, the SMTP log information appears on the **Logs** tab of the Policy Server Administration page. You can modify the severity level of messages that are written to the SMTP log on the MPE configuration page. The default severity is WARN. See [Configuring Log Settings for Servers in a Cluster](#) to modify the settings.

The HTTP Log

The HTTP log contains all Hypertext Transfer Protocol (HTTP) messages sent by the MPE device. In SMPP or XML mode, the HTTP log information appears on the **Logs** tab of the Policy Server Administration page. You can modify the severity level of messages that are written to the HTTP log on the server configuration page. The default severity is WARN. See [Configuring Log Settings for Servers in a Cluster](#) for more information.

Configuring Log Settings for Servers in a Cluster

To configure the log settings for the servers in a cluster:

1. From the **Policy Server** section of the navigation pane, select **Configuration**.

The content tree displays a list of server groups; the initial group is **ALL**.

2. From the content tree, select the **ALL** group.

The Policy Server Administration page opens in the work area.

3. Select an MPE device from the list.

The Policy Server Administration page opens in the work area and details the configuration settings of the selected device.

4. Select the **Logs** tab.

The Policy Server Administration page opens and details the logs configuration settings for the specified device.

5. To edit the logs configuration settings, click **Modify**.

The editable fields open in the work area.

6. In the **Modify Trace Log Settings** section of the page, select the **Trace Log Level** from the list.

This setting indicates the minimum severity of messages that are recorded in the trace log. These severity levels correspond to the syslog message severities from RFC 3164 *The BSD syslog Protocol*. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the trace log. The levels are:

- **Emergency**
Provides the least amount of logging, recording only notification of events causing the system to be unusable.
- **Alert**
Action must be taken immediately in order to prevent an unusable system.
- **Critical**
Events causing service impact to operations.
- **Error**
Designates error events which may or may not be fatal to the application.
- **Warning (default)**
Designates potentially harmful situations.
- **Notice**
Provides messages that may be of significant interest that occur during normal operation.
- **Info**
Designates informational messages highlighting overall progress of the application.
- **Debug**
Designates information events of lower importance.

Caution: Before changing the default logging level, consider the implications. Lowering the log level setting from its default value (for example, from **Warning** to **Info**) causes more notifications to be recorded in the log and can adversely affect performance. Similarly, raising the log level setting (for example, from **Warning** to **Alert**) causes fewer notifications to be recorded in the log and may cause you to miss important notifications.

7. You can enable and configure **Trace Log Forwarding Settings** for individual clusters.

Note: The CMP system provides log forwarding configuration for all products that have trace logs: MPE, MA, BoD, and the CMP itself.

For each cluster, enter the following:

- a. Select to enable **Enable Trace Log Forwarding** in the **Modify Trace Log Forwarding Settings** section of the page.

The Trace Log Forwarding settings become editable.

- b. Enter a valid **Hostname/IP Address** for each device receiving the trace logs.

Note: The system validates the IP address is unique based on the literal value. It does not resolve the host name or check the short pattern IPv6 to the full pattern IPv6 address.

- c. Select the appropriate **Severity** level for the trace logs being forwarded for each cluster. See [Step 6](#) for a description of each level.
8. In the **Modify Policy Log Settings** section of the page, configure the **Policy Log Level**.

This setting indicates the minimum severity of messages that are recorded in the policy log for all policies. The levels are:

- **OFF**
No messages are recorded.
- **DEBUG**
All messages are recorded.
- **INFO**
Only informational messages are recorded.
- **WARN (default)**
Only messages designating potentially harmful situations are recorded.

9. In the **Modify CMPP Log Settings** section of the page configure the **CMPP Log Level**.

This setting indicates the minimum severity of messages that are recorded in the CMPP log. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the CMPP log. The levels are:

- **OFF**
Turns off logging.
- **ERROR**
Designates error events which may or may not be fatal.
- **WARN (default)**
Designates potentially harmful situations.

- **INFO**
Designates informational messages highlighting overall progress.
- **DEBUG**
Designates information events of lower importance.
- **TRACE**
Designates informational events of very low importance.
- **ALL**
Records all logging levels.

10. In the **Modify SMPP Log Settings** section of the page, configure the following:

- a. **SMPP Log Level**—Indicates the severity of messages that are written to the file `SMPP.log`.

Adjusting this setting allows any new events, at or above the configured severity, to be written to the SMPP log.

Note: You can optionally enable the syslog forwarding address for new logs.

Valid levels are:

- **OFF**
Turns off logging.
 - **ERROR**
Designates error events which may or may not be fatal.
 - **WARN (default)**
Designates potentially harmful situations.
 - **INFO**
Designates informational messages highlighting overall progress.
 - **DEBUG**
Designates information events of lower importance.
 - **TRACE**
Designates informational events of very low importance.
 - **ALL**
Records all logging levels.
- b. **SMPP Log Forwarding IP Addresses**—Enter addresses for forwarding. You can forward SMPP log entries to multiple syslog servers.

11. In the **Modify SMTP Log Settings** section of the page, configure the **SMTP Log Level**.

This setting indicates the minimum severity of messages that are recorded in the SMTP log. These severity levels correspond to the syslog message severities from RFC 3164 *The BSD syslog Protocol*. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the SMTP log. The levels are:

- **OFF**
Turns off logging.
- **ERROR**
Designates error events which may or may not be fatal.
- **WARN (default)**
Designates potentially harmful situations.
- **INFO**
Designates informational messages highlighting overall progress.
- **DEBUG**
Designates information events of lower importance.
- **TRACE**
Designates informational events of very low importance.
- **ALL**
Records all logging levels.

12. In the **Modify HTTP Log Settings** section of the page, configure the **HTTP Log Level**.

This setting indicates the minimum severity of messages that are recorded in the HTTP log. Adjusting this setting allows new notifications, at or above the configured severity, to be recorded in the HTTP log. The levels are:

- **OFF**
Turns off logging.
- **ERROR**
Designates error events which may or may not be fatal.
- **WARN (default)**
Designates potentially harmful situations.
- **INFO**
Designates informational messages highlighting overall progress.
- **DEBUG**
Designates information events of lower importance.
- **TRACE**
Designates informational events of very low importance.
- **ALL**

Records all logging levels.

13. Click **Save**.

The log settings are configured.

Activity Logs per Subscriber

Note: Policy Management release 10.4.2 does not support this feature.

You can enhance the Policy Management monitoring capability by enabling users to input a subscriber ID that allows a log to capture all subscriber-related Policy device triggers and events received, policies evaluated and run, policy actions, and evaluations during the time frame defined while this Subscriber Activity Log is active.

Please refer to the appropriate *CMP User's Guide* for your system mode for more information about the Subscriber Activity Log.

Trace Log Notifications

This chapter lists Trace Log notifications. The incident ID number is also the Trace Log notification ID number. Trace Log notifications may have more than one severity. Each severity is listed with its applicable action. See [Viewing the Trace Log](#) for details.

Note: Trace log codes for all modes are represented in this list (cable, wireline, and wireless).

Expanded List

Note: The trace log number and title are derived from the Identifier and Defining Incident as defined in the system. Some trace log numbers and titles may be duplicated based on the system release and mode (that is, wireless, cable, or wireline).

1 – BoD TraceLog Init

Message

Initialized trace log.

Description

The CMP scheduler has initialized its interface to the trace log.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

2 – OSSI Collector Conn Establish

Message

OSSI collector establishing connection to *{type}*.

Description

The OSSI Collector is trying to connect to the specified database address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

3 – OSSI Collector Error

Message

Error occurred during OSSI collector run: *{type}*.

Description

The application that collects information from the OSS has experienced an error.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the OSS database is online and available.

4 – OSSI Collector Start

Message

Starting OSSI Collector run.

Description

The OSSI Collector task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

5 – OSSI Collector End

Message

OSSI Collector run completed.

Description

The OSSI Collector task has finished its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

6 – OSSI Collector Abort

Message

OSSI collector run aborted.

Description

The application that collects information from the OSS has been canceled due to user intervention.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

7 – OSSI Collector Config Read Error

Message

OSSI collector error reading configuration file: *{file name}*.

Description

The specified configuration file is not present or not readable.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8 – OSSI Collector Connection Success

Message

OSSI Collector established connection.

Description

The OSSI Collector has successfully connected to the OSS database.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

9 – OSSI Collector Connection Fail

MessageOSSI collector could not establish connection *{host name: port num}*.**Description**

The application that collects information from the OSS cannot connect to the specified OSS network element.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the OSS database is online and available.
2. If the problem persists, contact [My Oracle Support](#).

10 – OSSI Collector No CMTS Nodes

Message

OSSI collector did not find CMTS nodes for CMTS: *{name}*.

Description

The OSSI Collector did not find CMTS nodes for the specified CMTS.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

11 – OSSI Collector No Subs for CMTS

Message

OSSI collector did not find Subscribers for CMTS node: *{name}*.

Description

The OSSI Collector did not find subscribers for the specified CMTS node.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

12 – OSSI Collector Config Param Not Found

Message

OSSI collector did not find configuration parameter: *{parameter name}*.

Description

The specified parameter (for example, the host name, user name, or password) for the OSSI Collector task was not configured.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

13 – OSSI Collector Validate Error

Message

Error validating *{field}*.

Description

The OSSI Collector task retrieved a field from the OSS database that is invalid (for example, a malformed subnet address).

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check the field's value in the OSS database.

14 – DC Started

Message

Data Collector started.

Description

The Data Collector has initialized and started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

21 – Subnet SNMP Coll Task Start**Message**

Starting Subnet SNMP Collector task.

Description

The Subnet SNMP Collector task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

22 – Subnet SNMP Coll Task Timeout**Message**SNMP timeout while collecting *{1}* Subnet data from CMTS *{name}*.**Description**

The Subnet SNMP Collector task timed out.

The application requesting the specified subnet data from the network element did not receive a response from the specified network element.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the network element is online and available.

23 – Subnet SNMP Coll Task Error

Message

SNMP error *{type}* while collecting *{2}* Subnet data from CMTS *{name}*.

Description

The Subnet SNMP Collector task encountered an error.

The application requesting the specified subnet data from the identified network element received an unexpected response.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the network element is online and available.

24 – Subnet SNMP Coll Task Skip

Message

Skipping *{1}* Subnet collection from CMTS *{name}* because the SNMP community string is empty.

Description

The Subnet SNMP Collector task cannot poll the specified CMTS because the SNMP community string is not configured for it.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

25 – BOD Classifier Not Active

Message

Classifier not active for SUBIP={0}; SUBPORT={1}; DESTIP={2}; DESTPORT={3} - request ignored.

Description

The BoD Classifier for the specified subscriber IP address and port number is not active for the subscriber. The request was ignored.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

26 – BOD Classifier Active Exit Sub IP

Message

Classifier already active for EXTSUBIP={0}; EXTSUBIPMASK={1};
EXTSUBPORTSTART={2}; EXTSUBPORTEND={3}; EXTDESTIP={4};
EXTDESTIPMASK={5}; EXTDESTPORTSTART={6}; EXTDESTPORTEND={7}

Description

The BoD Classifier is already active for the specified exit subscriber IP address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

38 – Subnet SNMP Collector Task Status

Message

Subnet SNMP Collector Task Status CMTSs Processed: {num} Failures: {num} Subnets
Discovered: {num} Added: {num} Updated: {num} Removed: {num} Elapsed time:
{time} sec.

Description

The number of CMTSes processed and the number of subnets discovered by the
Subnet SNMP Collector task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

39 – Subnet SNMP Collector Task End**Message**

Finishing Subnet SNMP Collector task.

Description

The Subnet SNMP Collector task finished its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

41 – DC SNMP Collector Start**Message**

Starting Service Class Snmp Collector task.

Description

The Service Class SNMP Collector task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

42 – DC Collect Timeout

Message

SNMP timeout while collecting Service Class data from CMTS *{name}*.

Description

The application requesting the service class data from the network element did not receive a response from the identified network element.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the network element is online and available.

43 – DC Collect Error

Message

SNMP error *{type}* while collecting Service Class data from CMTS *{name}*.

Description

The application requesting the service class data from the network element received an unexpected response.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the network element is online and available.

44 – DC Empty Community

Message

Skipping Service Class collection from CMTS *{name}* because the SNMP community string is empty.

Description

The Service Class SNMP Collector task cannot poll the specified CMTS because the SNMP community string is not configured for it.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

50 – BOD HTTP Request Success

Message

HTTP request success: *{ip address}*

Description

The **BoD** HTTP request was successful for the specified IP address.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

58 – DC SNMP Collector Status

Message

Service Class Snmp Collector Task Status CMTSs Processed: *{num}* Failures: *{num}*
Service Classes Discovered: *{num}* Added: *{num}* Updated: *{num}* Removed: *{num}*
Elapsed time: *{time}* sec.

Description

The number of CMTSes processed and the number of service classes discovered by the Service Class SNMP Collector task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

59 – DC SNMP Collector Stop

Message

Finishing Service Class Snmp Collector task.

Description

The Service Class SNMP Collector task finished its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

61 – SNMP Collector Task Start

Message

Starting Subscriber Snmp Collector task.

Description

The Subscriber SNMP Collector task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

62 – SNMP Timeout

Message

SNMP timeout while collecting Subscriber data from CMTS *{name}*.

Description

The application requesting the subscriber data from the network element did not receive a response from the identified network element.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the network element is online and available.

63 – SNMP Error

Message

SNMP error *{type}* while collecting Subscriber data from CMTS *{name}*.

Description

The application requesting the subscriber data from the network element received an unexpected response.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the network element is online and available.

64 – Invalid Cable Modem MAC

Message

Invalid cable modem MAC address *{MAC address}* retrieved from CMTS *{name}*.

Description

The Subscriber SNMP Collector task retrieved an invalid cable modem IP address from the CMTS.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check the field's value in the network element.

65 – Invalid Cable Modem IP

Message

Invalid cable modem IP address *{ip address}* for **MAC** *{mac address}* retrieved from CMTS *{name}*.

Description

The Subscriber SNMP Collector task retrieved an invalid cable modem IP address from the specified CMTS.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check the field's value in the network element.

66 – Invalid CPE IP

Message

Invalid CPE IP address *{IP address}* behind cable modem *{MAC address}* retrieved from CMTS *{name}*.

Description

The Subscriber SNMP Collector task retrieved an invalid CPE IP address for the specified cable modem from the CMTS.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check the field's value in the network element.

68 – SNMP Community Empty

Message

Skipping Subscriber collection from CMTS *{name}* because the SNMP community string is empty.

Description

The Subscriber SNMP Collector task cannot poll the specified CMTS because the SNMP community string is not configured for it.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

70 – BOD SOAP Request Failure

Message

SOAP request failure: *{0}*

Description

The specified SOAP request failed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

78 – SNMP Collector Task Status

Message

Subscriber Snmp Collector Task Status CMTSs Processed: *{num}* Failures: *{num}*
Accounts Discovered: *{num}* Added: *{num}* Updated: *{num}* Removed: *{num}* Elapsed
time: *{time}* sec.

Description

The number of CMTSes processed and the number of accounts discovered by the
Subscriber SNMP Collector task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

79 – SNMP Collector Task End

Message

Finishing Subscriber Snmp Collector task.

Description

The Subscriber SNMP Collector task finished its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

80 – BOD SOAP Request Success**Message**

SOAP request success: {0}

Description

SOAP request is successful for the specified IP address.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

81 – DC CMTS Distributor Task Start**Message**

Starting CMTS Distributor task.

Description

The CMTS Distributor task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

82 – DC CMTS Error

Message

Error while sending CMTS data to Policy Server: *{name}*

Description

The CMP server cannot connect to the specified policy server to push the network element data.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

98 – DC CMTS Distributor Task Status

Message

CMTS Distributor Task Status Policy Server: *{name}* CMTS processed: *{num}* Added: *{num}* Updated: *{num}* Removed: *{num}* Elapsed time: *{time}* sec.

Description

The number of CMTSes processed by the CMTS Distributor task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

99 – DC CMTS Distributor Task Stop**Message**

Finishing the CMTS Distributor task.

Description

The CMTS Distributor task finished its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

100 – BOD Conn**Message**Established policy server connection to *{ip address}*

Description

A successful connection was established to the Policy Server at the specified IP address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

101 – Sub Distributor Task Start

Message

Starting Subscriber Distributor task.

Description

The Subscriber Distributor task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

102 – Sub Distributor Task Delete Error

Message

Error while deleting Subscriber data from Policy Server: *{name}*

Description

The CMP server cannot connect to the specified policy server to modify the subscriber data.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

103 – Sub Distributor Task Update Error

Message

Error while updating CMTS data on Policy Server: *{name}*

Description

The CMP server cannot connect to the specified Policy Server to modify the network element data.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

104 – Sub Distributor Task Send Reconfig Error

Message

Error while sending "Reconfigure" message to Policy Server: *{name}*

Description

The CMP server cannot communicate a new configuration for the specified Policy Server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

105 – Sub Distributor Task Send Refresh Chann Error

Message

Error while sending "Refresh Channels" message to Policy Server: *{name}*

Description

A communication problem occurred between the CMP server/Management Agent and the specified Policy Server during a data refresh of a channel information change request.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

106 – Sub Distributor Task Send Refresh Acct Error**Message**Error while sending "Refresh Accounts" message to Policy Server: *{name}***Description**

The Subscriber Distributor task request for a change to account information failed to send to the specified Policy Server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

107 – Sub Distributor Task Send Tier Error**Message**Error while sending Tier data to Policy Server: *{name}***Description**

The subscriber/account tier information configured in the CMP server did not push successfully to the specified Policy Server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

108 – Sub Distributor Task Send Channel Error

Message

Error while sending Channel data to Policy Server: *{name}*

Description

The CMP server experienced an error while sending channel information for a respective network element to the specified Policy Server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the policy server is online and available.

118 – Sub Distributor Task Status

Message

Subscriber Distributor Task Status CMTSs: {num} Accounts processed: {num} Added: {num} Updated: {num} Removed: {num} Elapsed time: {time} sec.

Description

The number of CMTSes and accounts processed by the Subscriber Distributor task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

119 – Sub Distributor Task End**Message**

Finishing Subscriber Distributor task.

Description

The Subscriber Distributor task finished its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

121 – OSSI Distributor Task Start

Message

Starting OSSI Distributor task.

Description

The OSSI Distributor task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

122 – OSSI Distributor Task Error

Message

Error occurred during OSSI Distributor run: *{type}*

Description

Failed to send data to the Management Agents.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

123 – OSSI Distributor Task Abort**Message**

OSSI Distributor run aborted

Description

A user canceled the distribution of the OSS information within the CMP server to the appropriate Management Agents.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

124 – OSSI Distributor Task Remote MA Error**Message**Error connecting to Remote MA: *{host name}***Description**

The CMP server could not establish a connection to the specified Management Agent.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the Management Agent is online and available.

125 – OSSI Distributor Task Update Acct Error

Message

Error updating Accounts to remote MA: *{host name}*

Description

The CMP server cannot connect to the specified Management Agent in order to update account information.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the Management Agent is online and available.

126 – OSSI Distributor Task Update CMTS Error

Message

Error updating CMTSs to remote MA: *{host name}*

Description

The CMP server cannot connect to the specified Management Agent to update the network element information.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the Management Agent is online and available.

127 – OSSI Distributor Task Update Tiers Error

MessageError updating Tiers to remote MA: *{host name}***Description**

The CMP server cannot connect to the specified Management Agent to update the subscriber tier information.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the Management Agent is online and available.

128 – OSSI Distributor Task Update Entitle Error

MessageError updating Entitlements to remote MA: *{host name}*

Description

The CMP server cannot connect to the specified Management Agent to update subscriber entitlement information.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the Management Agent is online and available.

139 – OSSI Distributor Task End

Message

Finishing OSSI Distributor task.

Description

The OSSI Distributor task is completing a scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

141 – CMTS MA Collector Task Start

Message

Starting CMTS MA Collector task.

Description

The CMTS MA Collector task is starting its run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

142 – CMTS MA Collector Task Error

Message

Error while collecting CMTS data from Management Agent: *{name}*

Description

The CMP server cannot collect the assigned network element information from the specified Management Agent.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check that the Management Agent is online and available.

157 – CMTS MA Collector Task Status MAS

Message

CMTS MA Collector Task Status# MA: {num}# CMTS processed: {num} Updated: {num} Skipped: {num}# Elapsed time: {time} sec.

Description

The CMP displays the CMTS MA Collector task status.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

158 – CMTS MA Collector Task Status CMTS

Message

CMTS MA Collector Task Status MAs processed: {num} Failed: {num} CMTS processed: {num} Updated: {num} Skipped: {num} Elapsed time: {time} sec.

Description

The CMTS MA Collector task results are displayed.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

159 – CMTS MA Collector Task End**Message**

Finishing CMTS MA Collector task.

Description

The CMTS MA Collector task is ending.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

161 – PCMM Dist Task Start**Message**

Starting PCMM Routing Distribution Task.

Description

The PCMM routing distribution task is starting.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

177 – PCMM Dist Task MPE Status

Message

Pcmm Distribution Task MPE Status# MPE: {n}# Status: {num}#

Description

The PCMM distribution task displays the status of the MPE device.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

178 – PCMM Dist Task Status

Message

Pcmm Distribution Task Status# MPEs processed: {num}# Updated: {num}# Failed: {num}# Elapsed time: {time} sec.

Description

The PCMM Distribution task processed the indicated number of MPE devices, updated the specified number, and encountered the specified number of failures within the indicated elapsed number of seconds.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specific cause.

179 – PCMM Dist Task End

Message

Finishing PCMM Routing Distribution task.

Description

The PCMM routing distribution task is ending.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

180 – DC Manual Task Start

Message

Task "{task name}" was run manually.

Description

The operator ran the specified task manually.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the message indicates any failures, check the system logs for specified cause.

201 – Healthchecker Task Start

Message

Starting HealthChecker task.

Description

HealthChecker task is starting its run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

219 – Healthchecker Task End**Message**

Finishing HealthChecker task.

Description

Healthchecker task is completing its run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

220 – DC AlertAging Task Start**Message**

Starting AlertAging task.

Description

The AlertAging task is starting its run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

239 – DC AlertAging Task End

Message

Finishing AlertAging task.

Description

The AlertAging task is ending its run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

240 – OM Stats Task Start

Message

Starting OM Statistics task.

Description

The OM Statistics task is starting its scheduled run.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

241 – OM Stats Task Data Available**Message**

OM Statistics collection complete and data is available for request.

Description

Data has been saved and is available for OSSI requests, prior to final cleanup tasks.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

243 – OM Stats Task Missing MPE**Message**

OM Statistics Task was unable to connect to MPE. UID: {0} {1}

Description

The OM Statistics Task was unable to connect to the specified MPE using the specified UID.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

244 – OM Stats Task Missing Stats

Message

OM Statistics Task was unable to retrieve statistics from MPE: *{name}* at hostname: *{host name}*; Error: *{error msg}*

Description

The OM Stats task was unable to retrieve statistics from the specified MPE device at the specified host name and received the indicated error code.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

245 – OM Stats task Missing MPE DB

Message

OM Statistics Task was unable to retrieve MPE from the database. UID: {0}

Description

The OM Statistics task was unable to retrieve the specified MPE device from the database.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

247 – OM Stats Task Retrieve Error

Message

OM Statistics Task error detected while retrieving statistics from MPE: {name}. Request attempt: {num}

Description

The OM Statistics task encountered an error while retrieving data from the specified MPE device and indicates the number of attempted requests.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

248 – OM Stats Task Retrieve Fail

Message

OM Statistics Task failed to retrieve statistics from MPE: *{name}*. Request attempt: *{num}*

Description

The OM Statistics task failed to retrieve statistics from the specified MPE devices and indicates the number of attempted requests.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

249 – OM Stats Task Retrieve Incomplete

Message

OM Statistics Task retrieved an incomplete set of statistics from MPE: *{name}*. Request attempt: *{num}*

Description

The OM Statistics task retrieved an incomplete set of statistics from the specified MPE device and indicates the number of request attempts.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

250 – OM Stats Task Proxy Fail**Message**

OM Statistics Task failed to retrieve proxy from MPE: *{name}*. Request attempt: *{num}*

Description

The OM Statistics task failed to retrieve proxy data from the specified MPE device and indicates the number of request attempts.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

251 – OM Stats Task Retrieve Error2**Message**

OM Statistics Task error retrieving statistics from MPE: *{name}*. Request attempt: *{num}*
Error: *{error msg}*

Description

The OM Statistics task encountered the specified error while retrieving statistics from the specified MPE device and the number of request attempts.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

252 – BoD DB Backup Fail

Message

BoD Database backup failed. The reason is : {msg}

Description

The BoD database failed to backup for the specified reason.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

253 – BOD DB Backup Start

Message

BoD Database backup started.

Description

BoD Database backup has started.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

254 – BoD DB Backup End**Message**

BoD Database backup finished.

Description

The BoD Database backup has finished.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

256 – OM Stats Task Success

Message

OM Statistics Task completed successfully.

Description

The OM Statistics task completed successfully.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Collection Task

Recovery

1. No action required.

257 – OM Stats Task Warn

Message

OM Statistics Task completed with a warning.#{*message*}

Description

The OM Statistics Task completed with the specified warning message.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

258 – OM Stats Task Failed**Message**OM Statistics Task failed. *{msg}***Description**

The OM Statistics task failed with the indicated failure message.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

259 – OM Stats Task Finish**Message**

Finishing OM Statistics task.

Description

The OM Statistics task completed.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP, DC

Group

Data Collection Task

Recovery

1. No action required.

260 – BoD Cluster Reinit

Message

The BoD cluster has reinitialized. The indicated blade is now the primary.

Description

The BoD cluster has reinitialized. The indicated server is now the primary server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

261 – Bad WGET Status

Message

Bad wget exit status "*code*" for name "*device*"

Description

Invalid status occurred on exit from wget with status *code* for the specified device.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

276 – Stat Rsync Clean Task Success**Message**

Statistics Rsync Cleanup Task completed successfully.

Description

Statistics Rsync Cleanup task completed successfully.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

278 – Stat Rsync Clean Task Failed**Message**Statistics Rsync Cleanup Task failed.#{*error message*}**Description**

The Statistics Rsync Cleanup Task failed with the specified message.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

279 – Stat Rsync Cleanup Task Finish

Message

Finishing Statistics Rsync Cleanup Task.

Description

The Statistics Rsync Cleanup Task is finished.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

280 – Subscription Aging Task Start

Message

Starting Subscription Aging Task.

Description

The Subscription Aging Task is starting.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

289 – Subscription Aging Task End**Message**

Finishing Subscription Aging Task.

Description

The Subscription Aging Task is finishing.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

300 – BoD Send**Message**

Sending {0} to {1} {2}

Description

The BoD is sending the specified item to the specified locations.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

301 – BoD Received Debug

Message

Received *{msg}* from *{host name}* {2}

Description

The BoD has received the specified message from the specified origin host.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

302 – BoD Request Timed Out

Message

{0} request to {1} timed out

Description

The specified request to the specified element has time out.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

303 – Quota Aging Task Start

Message

Starting Quota Aging Task.

Description

Starting quota aging task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

304 – Quota Aging Task End

Message

Finishing Quota Aging Task.

Description

The Quota Aging Task is finishing.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

310 – BOD XML Syntax Error PCM

Message

Incorrect XML syntax in PCMM services file *{file name}* *{error msg}*

Description

Incorrect XML syntax in PCMM

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

311 – BOD Missing Service Fields**Message**

Missing required fields for services {0}# Details: #{1}

Description

Missing required fields for services.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

312 – BOD XML Syntax Error**Message**

Incorrect XML syntax in Diameter services file {file name}#{1}

Description

The specified Diameter services file contains incorrect XML syntax.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

313 – BOD Service Index Exists

Message

Services or service indexes already exists # Details:#{0}

Description

Services or service indexes already exists.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

314 – BOD Same Service Mult Times

Message

Same services or service indexes used multiple times #Details:#{0}

Description

The same services or service indexes are used multiple times.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

400 – BOD MAC Translate Conn Fail

Message

MAC Translation failed due to connection failure for session ID *{num}*: MAC address: *{MAC address}* *{2}*.

Description

MAC Translation failed due to connection failure

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

401 – Stats Files Gen Task Start

Message

Starting Stats Files Generator Task.

Description

Starting Stats Files Generator Task in the DC process, which generates stats files from OSSI query.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

402 – Stats File Gen Task Success

Message

Stats Files Generator Task completed successfully.

Description

Stats Files Generator Task was completed successfully in the DC process.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

403 – Stats File Gen Task Failed

Message

Stats Files Generator Task failed. *{#1, 2, 3, or 4}*

Description

Error log indicating stats files generator task #1, 2, 3, or 4 failed. A Warning trace log is generated for troubleshooting.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Use the content of the Trace Log to troubleshoot the error.

404 – Stats File Gen Task Finish

Message

Finishing Stats Files Generator task.

Description

Info log generated at the completion of a stats files generator task. To verify these stat files, navigate to the local repository defined in this task configuration.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

405 – Stats File Gen Task Not Execute

Message

Stats Files Generator Task was not executed successfully.# There is not an enabled and non-empty Host Name/IP Address of Stats Files Synchronization Task.

Description

Stats Files Generator Task was not executed successfully.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

406 – Stats File Gen Task Fail Sync Blade

Message

Sync utility failed to sync stats files to mates. Reason: *#{reason}*

Description

Error log generated when the synchronize utility failed to synchronize stats files to mates. The reason for failure is listed in the log message.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Based on the failure message, check the server exchange SSH Key in CMP site1 Cluster and site2 Cluster.
2. Check the network connection status to other servers in both Clusters.

407 – Stats File Gen Task Fail Delete File**Message**

{task name} Task has removed some files which were not synced to remote servers{1}

Description

Warning log generated when a stats files generator task has removed some files which were not synchronized to remote servers, which includes remote server IP address. Stats files are kept for the period of time defined in the task setting. If these stats files have always been synchronized to the remote server, this task raises a Warning trace log.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check status of starting stats files synchronization #1,2,3,and 4, and ensure the Enabled stats were configured normally and successfully.

408 – Stats File Gen Task Fail NoStatsType**Message**

Stats Files Generator Task was not configured any stats type.

Description

Stats Files Generator Task was not configured for any stats type.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Configure the Stats File Generator.
2. If the problem persists, contact [My Oracle Support](#).

500 – BoD RDR Service Start Msg Received

Message

RDR: Start message received for Service Index *{index}*.

Description

RDR: Start message received for indicated Service Index.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

RDR

Group

RDR

Recovery

1. No action required.

501 – BoD RDR Unmapped Skip

Message

RDR: Skipping unmapped RDR, Service Index: *{index}* from *{1}*.

Description

BOD RDR Unmapped Skip

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

502 – Stats Sync Task Success

Message

{task num} Task completed successfully.

Description

Info log generated upon the successful completion of the stats files synchronization for task. The task name number (1 to 4) indicates different synchronization tasks.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

503 – Stats Sync Task Fail

Message

{task num} Task failed.#{1}

Description

Error log generated when stats files synchronization task fails; cause of failure is listed in log title. The task name and number (1 to 4) indicates the synchronization task during which the failure occurred.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Use content of trace log to troubleshoot error.

504 – Stats Sync Task End

Message

Finishing *{task num}* Task.

Description

Info log generated when the stats files synchronization process has finished.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

505 – Stats Sync Task Repository Missing

Message

The Local Repository does not exist, you need to check whether Stats Files Generator Task was executed successfully or not.

Description

Error log generated when the local repository does not exist; check whether stats files generator task was executed successfully or not.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Determine whether or not the stats files generator task was executed.

506 – Stats Sync Task Repository Fail

Message

{task num} Task still failed for sync local repository to remote server(*{host name}*) after retry *{num}* times

Description

Error log generated when a stats file synchronization task fails to synchronize a local repository to a remote server after three retries.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Determine if the remote server supports an SSH protocol connection.
2. Check the network connection status of the remote server.

507 – BoD Start Msg Processing Warn

Message

RDR: Start message processing *{0}*

Description

Warning log generated when a stats files synchronization task successfully synchronizes the local repository to a remote server after two retries.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. Check the network connection status of the remote server.

508 – BOD RDR Parse Fail

Message

RDR: Parsing Failed: *{id}* from *{rdr}*

Description

RDR failed to parse the indicated ID from the specified RDR.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

509 – BoD Drop RDR Service

Message

RDR: Dropping RDR *{error message}*, Service Index: *{index}* from *{RDR}*

Description

The BoD dropping the RDR Service with the indicated error.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

510 – BoD RDR Service Stop Msg Received

Message

RDR: Stop message received for Service Index *{index}*.

Description

RDR received a Stop message for the indicated Service.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

512 – BoD Drop RDR Bucket

Message

RDR: Dropping RDR *{error msg}*, Bucket Id: *{num}* from *{RDR}*

Description

RDR is dropping RDR with the indicated error.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

513 – BoD RDR Unmapped Skip2**Message**RDR: Skipping unmapped RDR, Bucket Id: *{id}* from *{rdr}*.**Description**

The BoD is skipping the indicated unmapped RDR.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

514 – BoD RDR Quota Msg Received**Message**RDR: Quota message received for Bucket Id *{id}*.**Description**

A Quota message was received for the specified Bucket ID.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

Data Collection Task

Recovery

1. No action required.

515 – BoD RDR Quota Msg Processing Warn | Info | Debug

Message

RDR: Quota message processing *{bucket id}*

Description

A Quota message is processing for the specified Bucket ID.

Severity

Debug, Info, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

RDR

Group

RDR

Recovery

1. If the problem persists, contact [My Oracle Support](#).

550 – XML Request Initiated

Message

OSSI XML Interface request initiated by: *{user name}*

Description

OSSI XML Interface request initiated by the specified user.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No action required.

552 – Account Send Error

MessageError while sending Account data to Policy Server: *{name}***Description**

An error occurred while sending Account data to the specified Policy Server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Subscriber

Recovery

1. If the message indicates any failures, check the system logs for specific cause.
2. If the problem persists, contact [My Oracle Support](#).

553 – XML Export Results

MessageFile *{type}* Export executed by *{user name}*. # Status: *{status}* # Total: *{num}* xml files**Description****Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No action required.

554 – XML Export Failure

Message

File *{type}* Export executed by *{user name}*. # Status: *{status}* # Failure Log Message:*{failure message}*

Description

OSSI XML export status for the indicated file type, exported by the indicated user.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No action required.

555 – XML Request Complete

Message

OSSI XML Interface request completed in *{mm:ss}* by:*{user name}*. {2}

Description

The completion of a user request to the XML Interface.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No action required.

620 – Push Init**Message**

Push of pending account updates initiated by: *{user name}*

Description

The specified user initiated account updates.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Subscriber

Recovery

1. No action required.

621 – Push Done

Message

Push of pending account updates completed by: *{user name}* *#{status}* #Total execution time *{time}*

Description

The push of pending accounts was completed with the specified status within the indicated time.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Subscriber

Recovery

1. No action required.

625 – Subscriber Acct Start

Message

Reapply of subscriber accounts initiated by *{user name}* for MPE *{name}*

Description

The indicated user initiated a reapply of subscriber accounts.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Subscriber

Recovery

1. No action required.

626 – Subscriber Acct End**Message**

Reapply of subscriber accounts completed by *{user name}* for MPE *{name}* *{status}* Total execution time *{time}*

Description

Reapply of subscriber accounts completed.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Subscriber

Recovery

1. No action required.

653 – RC Apply Change**Message**

Apply change of *{1}* to MPE(HostName:*{host name}*) From *{2}* to *{3}*

Description

Configuration change was applied to the specified MPE device.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Configuration

Recovery

1. No action required.

1001 – CMTS Conn Lost Clear

Message

PCMM: Established connection to *{id}*,

Description

A new PCMM connection was established to the specified CMTS or downstream policy server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1002 – CMTS Conn Lost

Message

PCMM: Lost connection to *{id}*

Description

The connection was lost to the specified CMTS or downstream policy server.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

N/A

Recovery

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, make sure the network path from the MPE device to the element (port 3918) is operational.
4. If the problem persists, contact [My Oracle Support](#).

1003 – AM Conn Lost Clear**Message**PCMM: Connection accepted from AM {*id*}**Description**

A new PCMM connection was accepted from the specified Application Manager or upstream policy server (that is, PCMM Router).

Note: Because of protocol limitations, the MPE device cannot distinguish between an AM and a PCMM router, so it always identifies the incoming connection as an AM.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery

1. No action required.

1004 – AM Conn Lost Set

Message

PCMM: Lost connection with AM *{id}*

Description

The MPE device lost a connection from the specified application manager (AM) or upstream policy server (that is, a PCMM router).

Note: Because of protocol limitations, the MPE device cannot distinguish between an AM and a PCMM router, so it always identifies the incoming connection as an AM.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

PCMM

Recovery

1. Check the availability of the AM.
2. Check the AM log for a recent failover or other operations that can interrupt communications.
3. If the AM has not failed, make sure the path from the AM to the MPE device (port 3918) is operational.
4. If the problem persists, contact [My Oracle Support](#).

1010 – PCMM Received AM

Message

PCMM:Received *{msg type}* from AM *{id}* *{msg contents}*

Description

This trace log records every received message in both MPE-R and MPE-S devices. If the MPE device receives the PCMM requests containing the CMTSIP field, the CMTSIP is also recorded in this trace log. The PCMM requests may be GateSet | GateInfo | GateDelete.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. No action required.

1011 – PCM Send**Message**

PCMM: Sending *{msg type}* to *{id}* *{msg contents}*

Description

The specified message type was sent to the specified CMTS (or downstream policy server).

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. No action required.

1012 – PCM Receive Warn

Message

PCMM: Received *{msg type}* from *{id}* *{msg contents}*

Description

The specified message type was received from the specified CMTS (or downstream policy server).

Note: This message is logged at the Warning level when the PCMM message is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1013 – PCM Send AM Warn

Message

PCMM: Sending *{msg type}* to AM *{id}* Details: *{msg contents}*

Description

The specified message type was sent to the specified AM (or upstream policy server).

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1014 – PCMM Fail Send Message Error

MessagePCMM: Failed (*{num}* attempts) to send *{msg type}* event message to *{id}* *{3}***Description**

A PCMM event message could not be transmitted to the specified record keeping server (RKS).

Note: The last attempt that fails is logged as an Error. If there are additional retries to be attempted then this is logged as a Warning.

Severity

Warning, Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. Check the configuration and availability of the RKS.
2. Ensure the network path from the MPE device to the RKS is available.

1015 – PCMM Success Send Message

MessagePCMM: Successfully sent *{msg type}* event message to *{id}* *{msg contents}*

Description

A PCMM event message was successfully sent to the specified RKS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. No action required.

1016 – PCMM Fail Over RKS

Message

PCMM: Failover initiated for RKS *{id}*, reverting to *{id}*

Description

The system has lost communication with the primary RKS, and is attempting to establish a connection with the secondary RKS. The identities of both the primary and secondary RKSs are specified.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. Check the configuration and availability of the RKS.

2. Ensure the network path from the MPE device to the RKS is operational.

1017 – PCMM Fail Too Busy

Message

PCMM: Failed (TOO BUSY) to send *{msg type}* event message to *{id}* *{msg contents}*

Description

The MPE device is unable to send an event message to the specified RKS because the send queue is full.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. This is normal behavior under heavy PCMM load. It can also occur if there is a communication problem with the RKS because the send queue may fill while the retry messages are being sent.

1020 – PCM Reject No PEP

Message

PCMM: Rejecting *{msg type}* - no PEP available for SubId *{ip address}*

Description

A PCMM message was received with the specified subscriber IP address but there is no configured CMTS (or downstream policy server) to handle this request.

Note: The request will be rejected with a PCMM error code of 13 (Invalid SubscriberID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. Check the configuration of the CMTSes associated with this MPE device. Make sure that there is a CMTS configured with a subnet for the specified subscriber AND make sure that this CMTS is associated with this MPE device.
2. Check the configuration of the AM sending the message to make sure it is sending the request to the correct MPE device.

1021 – PCMM Reject Invalid Gate

MessagePCMM:Rejecting *{msg type}* - invalid gate id *{gate ID}***Description**

A PCMM message was received with a Gate ID that does not correspond to any sessions in the MPE database. This checking is only performed if the CMP server has Validate the gate ID enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 2 (Unknown GateID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the flow of messages between the AM, the MPE device, and the CMTS to determine if there are errors in the message forwarding.

1022 – PCMM Reject AMID Mismatch

Message

PCMM: Rejecting *{msg type}* - AmId mismatch - request *{msg amid}* doesn't match gate *{mpe amid}*

Description

A PCMM message was received with an AMID that does not match the AMID for the corresponding session in the MPE database. This checking is only performed if the CMP system has Validate the application enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 14 (Unauthorized AMID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the flow of messages between the AM and the MPE device to determine if there are errors in the message processing.

1023 – PCMM Reject SubId Mismatch

Message

PCMM: Rejecting *{msg type}* - SubId mismatch - request *{msg sub id}* doesn't match gate *{mpe sub id}*

Description

A PCMM message was received with a Subscriber ID that does not correspond to a provisioned subscriber in the MPE database of known subscribers (CPEs). This

checking is only performed if the CMP system has Validate user enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 13 (Invalid SubscriberID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the flow of messages between the AM and the MPE device to determine if there are errors in the message processing.

1024 – PCMM Reject Unknown Subscriber

MessagePCMM:Rejecting {*msg type*} - Unrecognized Subscriber {*subID*}**Description**

A PCMM message was received with a Subscriber ID that does not correspond to a provisioned subscriber in the MPE database of known subscribers (CPEs). This checking is only performed if the CMP system has Validate user enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 13 (Invalid SubscriberID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the OSS system you are using to provision subscribers for the MPE device to make sure that this subscriber is provisioned.

1025 – PCMM Reject Unauth AMID**Message**PCMM: Rejecting *{msg type}* - Unauthorized AmId *{id}***Description**

A PCMM message was received with an AMID that does not correspond to any known application manager in the MPE device. This checking is only performed if the CMP system has Validate the application enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 14 (Unauthorized AMID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the application definitions in the CMP system and make sure that this AMID is associated with the appropriate application.

3. Make sure that the application is also associated with this MPE device in the CMP system.

1026 – PCMM Reject Unknown Service

Message

PCMM: Rejecting *{msg type}* - Unrecognized Service Class Name *{name}*

Description

A PCMM message was received with a Service Class Name that does not correspond to any service class that is known to exist for the CMTS to which this message is being sent. This checking is only performed if the CMP system has Validate the service class enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 11 (Undefined Service Class).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the set of Service Class names that are provisioned for the CMTS in the CMP system and make sure that the specified name is included.
3. Make sure the set of Service Class names in the CMP system is consistent with the set of values on the actual CMTS.
4. Make sure that the AM is sending the correct value.

1027 – PCMM Reject Incompat Envelop

Message

PCMM:Rejecting *{msg type}* - Incompatible Envelopes - *{env type}* ENV exceeds *{env type}* ENV

Description

A PCMM message was received with incompatible Authorized, Reserved and Committed envelopes (QoS parameter specifications). This checking is only performed in the CMP system has Validate traffic profile envelopes enabled for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 12 (Incompatible Envelope).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, disable it in the CMP system.
2. Check the configuration of the AM because this is an indication that it is requesting parameters that violate the protocol specification.

1028 – PCMM Reject Exceed CMTS Limit**Message**

PCMM: Rejecting *{msg type}* - Classifier count exceeds CMTS limit

Description

A PCMM message was received with more classifiers than the provisioned limit for the CMTS to which this message is being sent. This checking is performed only if the CMP system has set the configuration key, PCMM.Check.Classifiers, to true for the MPE device (by default this is off).

Note: The request will be rejected with a PCMM error code of 15 (Number of Classifiers not Supported).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If you do not want this checking to be performed, set the configuration key, PCMM.Check.Classifiers, to false in the CMP system. Refer to the *CMP User Guide* for details.
2. Check the Classifier Limit that is provisioned for the CMTS in the CMP system and make sure that it is consistent with the actual CMTS.
3. Make sure your AM is configured to make requests that do not exceed the CMTS limit.

1029 – PCMM Failed To Send Gate Message

Message

PCMM: Rejecting {msg type} - I/O Error while sending to {id}

Description

There was no PCMM session connection to the target CMTS (or downstream policy server).

Note: The request will be rejected with a PCMM error code of 255 and a subcode of 211.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

PCMM

Recovery

1. Check the network connectivity between systems.

1050 – Policy Reject2

Message

Rejecting *{msg type}* - Rejected by policy "*{name}*"

Description

The specified message was rejected by the specified policy rule.

Note: The request will be rejected with a PCMM error code of 255 and a subcode of 254.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

N/A

Recovery

1. Check the policy rule and the contents of the message to make sure it is operating as expected.
2. It may be helpful to increase the logging level of the policy log and then repeat this request to examine the details of the policy execution.
3. If the problem persists, contact [My Oracle Support](#).

1051 – Policy Reject

Message

Rejecting *{msg type}* - Rejected by policy "*{name}*"

Description

The specified message was rejected by the specified policy rule.

Note: The request will be rejected with a PCMM error code of 255 and a subcode of 254.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

N/A

Recovery

1. Check the policy rule and the contents of the message to make sure it is operating as expected.
2. It may be helpful to increase the logging level of the policy log and then repeat this request to examine the details of the policy execution.
3. If the problem persists, contact [My Oracle Support](#).

1101 – DQOS Downstream Connection Closed Clear | Set

Message

DQOS: Established connection to *{id}*

Description

A new connection was established to the specified CMTS or downstream policy server.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DQOS

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1102 – MSC Conn Lost | Lost Clear

Message

DQOS: Lost Connection to *{id}*

Description

The connection to the specified CMTS or downstream policy server was lost.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

DQOS

Recovery

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, make sure the network path from the MPE device to the element (port 3918) is operational.

1104 – DQOS AM Connection Closed Clear | Set

Message

DQOS: Lost connection with CMS *{id}*

Description

The MPE device lost a connection from the specified CMS.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

DQOS

Recovery

1. Check availability of the CMS.

1110 – DQOS Received CMS

Message

DQOS: Received *{msg type}* from CMS *{id}* *{2}*

Description

The specified message type was received from the specified CMS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DQOS

Recovery

1. No action required.

1111 – DQOS Sending

Message

DQOS: Sending *{msg type}* to *{id}*

Description

The specified message type was sent to the specified CMTS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DQOS

Recovery

1. No action required.

1112 – DQOS Received**Message**DQOS: Received *{msg type}* from *{id}* *{msg contents}***Description**

The specified message type was received from the specified CMTS.

Severity

Info, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DQOS

Recovery

1. This message is logged at the Warning level when the DQOS message is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

1113 - DQOS Send CMS Warn**Message**DQOS: Sending *{msg type}* to CMS *{id}*

Description

The specified message type was sent to the specified CMS.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DQOS

Recovery

1. This message is logged at the Warning level when the DQOS message is an error message such as GAteSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

1120 - DQOS Reject No CMTS

Message

DQOS: Rejecting *{msg type}* - no CMTS available for SubId *{ip address}*

Description

A DQOS message was received with the specified subscriber IP address but there is no configured CMTS to handle this request.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

DQOS

Recovery

1. Check the configuration of the CMTSes associated with this MPE device. Make sure that there is a CMTS configured with a subnet for the specified subscriber AND make sure that this CMTS is associated with this MPE device.

1121 – DQOS Reject Gate

Message

DQOS: Rejecting *{msg type}* - invalid gate id *{id}*

Description

A DQOS message was received with a Gate ID that does not correspond to any session in the MPE database. This checking is only performed if the CMP server has enabled Gate checking for the MPE device (by default this is off).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

DQOS

Recovery

1. If you do not want this checking to be performed, disable it in the CMP.

1123 – DQOS Reject Sub ID

Message

DQOS: Rejecting *{msg type}* - SubId mismatch - request *{msg id}* doesn't match gate *{mpe id}*

Description

A DQOS message was received with a Subscriber ID that does not match the Subscriber ID for the corresponding session in the MPE database. This checking is only performed if the CMP server has enabled Gate checking for the MPE device (by default this is off).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

DQOS

Recovery

1. If you do not want this checking to be performed, disable it in the CMP.

1124 – DQOS Reject Subscriber

Message

DQOS: Rejecting *{msg type}* - Unrecognized Subscriber *{id}*

Description

A DQOS message was received with a Subscriber ID that does not correspond to a provisioned subscriber in the MPE database of known subscribers (CPEs). This checking is only performed if the CMP server has enabled Subscriber checking for the MPE device (by default this is off).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

DQOS

Recovery

1. If you do not want this checking to be performed, disable it in the CMP.

1129 - DQOS Reject

Message

DQOS: Rejecting *{msg type}* - DQOS I/O Error while sending to *{id}*

Description

An unexpected I/O error was encountered while trying to send the specified message to a CMTS.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

DQOS

Recovery

1. Check the logs for further details on the I/O error.
2. Check the availability of the destination CMTS and the operational status of the network to the CMTS.

1150 - DQOS Policy Reject**Message**

DQOS: Rejecting {0} - Rejected by policy "{name}"

Description

The specified message was rejected by the specified policy rule.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

DQOS

Recovery:

1. Check the policy rule and the contents of the message to make sure it is operating as expected. It may be helpful to increase the logging level of the policy log and then repeat this request to examine the details of the policy execution.

1204 - SPC Conn Closed | Closed Clear

Message

SPC DQOS: Lost connection with CMS *{id}*

Description

The MPE device lost a connection from the specified **CMS**.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. Check availability of the CMS.
2. Check the CMS log for a recent failover or other operations that can interrupt communications.
3. If the CMS has not failed, make sure the path from the CMS to the MPE device (port 2126) is operational.

1209 - SPC DQOS Gate Delete

Message

SPC DQOS: Deleting gate *{gate id}*, T1 Timer expired

Description

The specified gate was deleted because it did not transition from the RESERVED state to the COMMITTED state before the T1 Timer expired.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. Check the logs and status in the CMS to determine why the gate did not get committed. This may be a normal situation in which the call was aborted before it was fully set up.

1210 - SPC DQOS Received**Message**SPC DQOS: Received *{msg type}* from CMS *{id}* *{msg contents}***Description**

The specified message type was received from the specified CMS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1213 - SPC DQOS Send CMS Warn**Message**SPC DQOS: Sending *{msg type}* to CMS *{id}*

Description

The specified message type was sent to the specified CMS.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1221 - SPC DQOS Global Session Reject

Message

SPC DQOS: Rejecting *{msg type}* - invalid global session id *{global sess id}*

Description

The MPE device received a request to perform an operation on a global session (call) that does not exist in the MPE database.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. This is usually an indication that there is a protocol error or communication problem between an MPE device and a CMS.

2. If there was a recent failover or communication interruption, it is possible that one of the devices may have data that is not complete.

1231 - SPC DQOS Ingress Reject

Message

SPC DQOS: Rejecting *{msg type}* - invalid ingress id *{ingress id}*

Description

The MPE device received a request to set up a gate for a zone that does not exist (as specified by the ingress ID in the request)

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. Ensure that the topology information in the MPE device is up-to-date and consistent with the topology information in the CMS that issued the request.

1232 - SPC DQOS Gate Reject

Message

SPC DQOS: Rejecting *{msg type}* - no path to root zone for ingress id *{ingress id}*

Description

The MPE device received a request to set up a gate for a zone that does not have a valid path to the root zone.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

SPC DQOS

Recovery:

1. Although in theory this is possible, it should not happen unless there is a problem in the configuration of the network topology. Verify that the network topology is defined correctly.

1233 - SPC DQOS Gate Drop

Message

SPC DQOS:Dropping *{msg type}* - invalid gate id *{gate id}*

Description

The MPE device received a request that referenced the specified gate ID and an unrelated session (via the GlobalSessionID).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. This is usually an indication that there is a protocol error or communication problem between an MPE device and a CMS.
2. If there was a recent failover or communication interruption, it is possible that one of the devices may have data that is not complete.

1250 - SPC DQOS Policy Reject

Message

SPC DQOS:Rejecting *{msg type}* - Rejected by policy "*{policy name}*"

Description

The specified request was rejected because of a policy rule (specified by policy name).

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

SPC DQOS

Recovery

1. This is usually an indication that a device in the path would have exceeded its capacity limit if the request had been approved. For more details check the Network Topology Viewer in the CMP server.

1370 - BRAS IP Declared Static**Message**

BRAS: COPS-PR declared an IP address (*{ip address}*) already defined as static in account *{account id}*

Description

A subscriber attached to the network with a static IP address, but the BRAS to which the subscriber is connected also assigned a dynamic IP address.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery:

1. Either remove the static IP definition or configure the subscriber on the BRAS to have a static IP address.

2. If the problem persists, contact [My Oracle Support](#).

1401 – Diam Conn Opened W Peer

Message

Diameter: Transport connection opened with peer *{ip address:port}*

Description

A transport level connection (such as TCP) has been established with the specified Diameter peer.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Diameter

Recovery

1. No action required.

1402 – Connectivity Lost | Lost Clear

Message

Diameter: Connectivity lost with peer *{host name}{(ip address)}, {new alarm | alarm cleared}*

Description

A connection with a peer has been closed/opened by peer.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Diameter

Recovery

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, ensure the network path from the MPE device to the element is operational.
4. Verify that the peer is online (although the connection can recover on its own on the next retry attempt).

1403 – Connectivity Degraded | Degraded Clear**Message**

Diameter: Connectivity degraded with peer *{host name}* (*{ip address}*), *{new alarm | alarm cleared}*

Description

A connection with a peer has degraded.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Diameter

Recovery

1. Verify that the peer is online (although the connection can recover on its own on the next retry attempt).

1404 – Send Message | Debug | Info**Message**

Diameter: Sent *{msg type [device name]}* to *{device name}* *{ip address}*

Description

A Diameter message has been sent to the specified peer using the specified connection. When the message contains an error, the event logs with a Warning; when the message processes normally, the event logs as Info; for Diameter Watchdog requests and answers, the event logs as Debug.

Severity

Warning, Info, Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. No action required.

1405 – Receive Message | Debug | Info

Message

Diameter: Received *{msg type [device name]}* from *{device name}* *{ip address}*

Description

A Diameter message has been received from the specified peer to the specified connection. When the message contains an error, the event logs with a Warning; when the message processes normally, the event logs as Info; for Diameter Watchdog requests and answers, the event logs as Debug.

Severity

Warning, Info, Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. No action required.

1406 – Receive Message EXC**Message**

Diameter: Error processing message *{msg}* from *{peer id}* *{conn id}*

Description

An error occurred while processing a received message from the specified peer over the specified connection.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. Check the error code and verify that the message received is properly formatted.

1407 – Peer Status Change Notice | Warn**Message**

Diameter: Peer *{name(ip address)}* status changed from *{INITIAL | OKAY}* to *{OKAY | DOWN}*

Description

The status of a Diameter peer has changed. This event is usually generated after a connection has been established and capability exchange has occurred (Notice level) or after a connection was torn down with a peer (Warning level).

Severity

Notice, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. If a Warning level, check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, ensure the network path from the MPE device to the element is operational.

1408 – New Conn Rejected | New Conn Rejected Clear**Message**

Diameter: New connection *{ip address:port}* rejected as a valid connection already exists with peer *{peer id}*[, alarm cleared]

Description

A Diameter peer (identified by its Diameter Identity) attempted to establish a connection with the Policy Management device although it already has a valid connection. The Diameter protocol allows only one connection from a particular peer.

Severity

Error/Info

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Diameter

Recovery

1. Check the peer configuration and ensure that from the peer's perspective, it also sees a valid connection with the MPE device.
2. If the problem persists, contact [My Oracle Support](#).

1409 – Reject Missing AVP

Message

Diameter: Rejecting *{msg type}* from *{peer id}* - *{conn id}* AVP(s) not found in request *{request details}*

Description

The request was rejected by the Policy Management device as it was missing an AVP that was required for the processing of the request based on the corresponding Diameter application procedures and current session state.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. Check the peer configuration to identify the reason the AVP was not included in the request.

1410 – Message Timeout

Message

Diameter: Response timeout for *{msg type}* sent to *{conn id}* *{msg details}*

Description

A response message was not received for the request sent to the destination host.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1411 – Duplicate Message

Message

Diameter: Received duplicate message *{msg type}* from *{conn id}* *{msg details}*

Description

The received message was discarded because it was received previously by another message containing the same Diameter End-to-End Identifier from the same origin host.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1412 – Send Response Info | Warn | Debug

Message

Diameter:Sent *{msg type}* to *{peer id}* in *{time}* ms *{msg details}*

Description

A Diameter message was sent.

Severity

Info, Warning, Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1413 – Receive Response Info |Warn | Debug**Message**Diameter: Received *{msg type}* from *{peer id}* in *{time}* ms *{msg contents}***Description**

A Diameter message was received.

Severity

Info, Warning, Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1414 - SCTP Path Status Changed | Changed Clear**Message**Diameter: SCTP path on association ID *{id}* address *{1}* *{2}***Description**

An SCTP path is unavailable. An Info level message is generated when a backup or non-primary path is confirmed by the SCTP association. An Error level message is generated when one of the paths fails, whether it is a primary or non-primary path. A Notice level message is generated when a path that previously failed recovers.

Severity

Notice, Error

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1415 - Diam CR Conn Opened W Peer

Message

ConnectionRouter: Diameter Connection established towards *{Primary MRA Identity (IP:port)}* for the peer *{NE identity (IP:port)}*.

Description

PCD Connection established between the secondary MRA and the primary MRA for the NE.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1416 - Diam CR Conn Disconnected W Peer

Message

ConnectionRouter: Diameter Connection created towards *{Peer Identity(IP:port)}* for the peer *{Peer Identity(IP:port)}* is now disconnected.

Description

PCD Connection disconnected between the secondary MRA and the primary MRA.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1417 - CR Message Forwarded

Message

ConnectionRouter: *{Message Type}* forwarded by Connection Router from *{Source Peer Diameter Identity(IP:port)}* to *{Destination Peer Diameter Identity(IP:port)}*.

Description

Message is forwarded from the External to Internal connection OR vice-versa.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1420 – Diam Reject No PCEF | Warn

Message

Diameter: Rejecting *{app function}* - no PCEF available for subscriber

Description

Request from an application function (such as P-CSCF) was rejected by the MPE device as there was no corresponding session with the PCEF (such as a GGSN) for the subscriber.

Severity

Error, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. Check the provided subscriber identification and IP address and verify that it corresponds to a subscriber who is attached to the network.

1421 – Diam Missing Profile For Media

Message

Diameter: No default QoS profile defined for media *{type}*

Description

The MPE device received a request (such as Rx) from an application to set up policy rules on the enforcement device, but the application function did not provide enough information in the request for the device to derive corresponding quality of service (QoS) parameters, and there are no default profiles configured in the device for the corresponding media type.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Check the MPE device configuration for Diameter AF default QoS profiles and add a default QoS profile for the media type in question.
2. Verify the reason why the application function did not provide enough info to the device within the application request.

1440 – Diam No Associated NE**Message**

Diameter: Rejecting request for subscriber *{sub id}* - No Network Element found for node *{node id}*

Description

The MPE device rejected a request (such as Gx) from an enforcement device (such as a GGSN) because it did not recognize it as a “known” network element.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Check the MPE device configuration and verify that the enforcement device is configured as a Network Element and associated with the MPE device.
2. Verify that the Network Element's Diameter identity is configured.

1441 – Rule Fail

Message

Diameter: PCC/ADC rule *{rule name}* failed for subscriber *{sub id}* *{2}* - Rule failure code *{fail code}*

Description

A PCEF Charging-Rule-Report indicated that installation of the specified **PCC/ADC** rule for the specified subscriber and Diameter session failed with the specified failure code. If the PCEF reports failure to install multiple rules for the same reason, the MPE device generates a single event with multiple rule names.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No actions are required.

1442 – Rule Retry

Message

Diameter: PCC/ADC rule *{rule name}* retry *{num}* of *{max num}*; RetryCycle *{num}* for subscriber *{sub id}* *{sess id}*. Next retry in *{time}* seconds.

Description

This event is generated by the MPE device when a PCC rule installation retry has been initiated as a result of a rule installation failure. This event will contain the name of the PCC rule, the retry attempt number and maximum retries (for example, “retry 1 of 3”), current Retry Cycle, the Diameter Session-Id, and subscriber identifier. If this is not the final retry attempt, the event will contain information about when the next retry will be attempted (for example, “next retry in 30 seconds”).

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No actions are required.

1443 – Retry Fail Error

Message

Diameter: PCC/ADC rule *{rule name}* retry failed after *{num}* attempts for subscriber *{sub id}* *{sess id}*

Description

This log entry is generated by the MPE device when a CCR-U with a Rule failure code and an RAR with a result code of either DIAMETER_PCC_RULE_EVENT (5142), DIAMETER_ADC_RULE_EVENT(5148), or DIAMETER_AN_GW_FAILED (4143) contained in the rule report triggers the last retry RAR attempt of the last retry cycle. The log entry contains the name of the PCC rule, the number of retry attempts (that is, maximum retry cycles * max retry attempts per cycle), the Diameter Session-Id, and the subscriber identifier.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If necessary adjust configuration values.

1444 – Rule Retry Canceled

Message

Diameter:PCC/ADC rule *{rule name}* retry canceled for subscriber *{sub id}* *{sess id}*

Description

Retrying installation of the specified PCC rule was canceled for the specified subscriber and Diameter session. This can happen because the rule was removed or installed as the result of a policy action. This log will contain the name of the PCC rule, the Diameter Session-Id and subscriber identifier.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No actions are required.

1445 – Rule Retry Error Too Many

Message

Diameter:PCC/ADC rule *{rule name}* retry aborted for subscriber *{sub id}* *{sess id}* - Too many retries in progress (*{num}* attempts)

Description

A rule installation retry cannot be initiated because the maximum number of simultaneous retries has been reached.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If necessary, adjust configuration values.

1446 – Max PDN Connections**Message**

Diameter: The maximum number of PDN connections per binding has been exceeded for subscriber *{sub id}*

Description

The maximum number of PDN connections has been exceeded for a subscriber.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. No actions are required

1447 – Diam Too Many Sessions**Message**

Diameter: The maximum number of secondary sessions has been exceeded for same IP-CAN session association for subscriber : *{sub id}*

Description

The maximum number of secondary sessions has been exceeded for the same IP-CAN session association for the specified subscriber.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

1450 – SCE GX No Profile

Message

SceGx:No SCE Profile or Default Profile set for subscriber {0} {1}

Description

For the specified subscriber, there was no **SCE** Package ID set using either an SCE Traffic Profile in policy or the Diameter **PCEF** Default Profile.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Ensure all subscribers have an SCE Traffic Profile applied to their CCR-I request, either using policy or by selecting an SCE Traffic Profile as the Diameter PCEF Default Profile.

1470 – Diam Session Cleanup Start

Message

Diameter: Starting cleanup task

Description

The Diameter session binding cleanup task has begun.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

1471 – Diam Session Cleanup Send RARs

Message

Diameter: Finished iterating the database. Starting to send RARs to *{num}* suspect sessions

Description

The database iterations (listing the potential number of stale sessions identified for cleanup) have ended.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

1472 – Diam Session Cleanup Complete

Message

Diameter: Completed session cleanup

Description

The diameter session binding cleanup task has ended and the purging process has started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

1473 – PCMM Session Cleanup Send GateInfos

Message

PCMM: Finished iterating the database. Starting to send GateInfos to *{num}* suspect sessions

Description

PCMM finished iterating the database. Starting to send GateInfos to suspect sessions.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CPE

Group

N/A

Recovery:

1. No action required.

1474 – PCMM Session Cleanup Start**Message**

PCMM: Starting cleanup task

Description

Cleanup task is starting

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery:

1. No action required.

1475 – PCMM Session Cleanup Complete**Message**

PCMM: Completed session cleanup

Description

PCMM finished session cleanup

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery

1. No action required.

1476 – Diam Session Cleanup Built Complete

Message

Diameter: Completed session cleanup list built

Description

Diameter finished building the session cleanup list.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery

1. No action required.

1477 – PCMM Session Cleanup Built Complete

Message

PCMM:Completed session cleanup list built

Description

PCMM finished building the session cleanup list.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery:

1. No action required.

1600 – DBPLUGIN No Match Warn**Message**

DBPLUGIN:No matches for {0}

Description

DbPlugin search request did not find any results for the specified criteria.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. No actions are required

1601 – LDAP Conn To

Message

LDAP: Established connection to *{server}*

Description

A new LDAP connection to the specified server was established.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required.

1602 – LDAP Closing Conn To

Message

LDAP:Closing connection to *{server}*

Description

The LDAP connection to the specified server was closed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required.

1605 – LDAP Conn Failed | Failed Clear

Message

LDAP: Attempted connection to *{ip address}:{port}* failed, reason: *{msg}*

Description

A connection attempt to the indicated server failed for the reason described in msg.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. Verify that there is not a problem with the LDAP server or the network path used to reach the server.
2. Check LDAP data source configuration to verify proper connection information is provided.

1610 – LDAP Search Fail

Message

LDAP:Search failure for *{id}* due to the following error: *{error msg}*

Description

LDAP search failure due to an error.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1611 – LDAP Search

Message

LDAP:Searching for *{stype}*: *{criteria}*

Description

A search is being performed for the search type *stype* using the specified criteria.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required.

1612 – LDAP Search Results

Message

LDAP:Search results for *{stype}* *{filter}* are: *{results}*

Description

Displays the results of the search request (if matches found).

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required.

1613 – LDAP Search No Matches**Message**LDAP:No matches for *{stype} {filter}***Description**

A search returned no results.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. With multiple data sources, an individual data source might not return any results.

1614 – LDAP Multi Match**Message**LDAP: Multiple matches for *{stype} {filter}***Description**

A search returned multiple results.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. Verify that the search criteria should have resulted in multiple matches. If necessary, correct the LDAP configuration.

1615 – LDAP Search Fail2

Message

LDAP:Unexpected search failure for *{stype} {filter}*, reason: *{msg}*

Description

A search was terminated because of an unexpected exception.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. Check the cause of the exception and check the LDAP configuration for any errors that might have caused the problem.

1617 – LDAP Modify Entry

Message

LDAP: Modify Entry for *{process id}: {key}*

Description

This is a detailed description of the LDAP modification to be initiated. Example – Modify Entry for *Processor ID* (for example *UserByE164*); LDAP Processor: *Processor ID*
Entry DN: *LDAP DN* Attribute: *LDAP Attribute* Value: *new value*

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No action required.

1619 – LDAP Modify Unexpected Error

Message

LDAP: Unexpected modify failure for *{process id} {key}*, reason: *{msg}*

Description

Unexpected LDAP modify failure.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1620 – LDAP Queue Distress

Message

LDAP: Operation queue *{process id}* in distress. Queue capacity exceeds *{event msg}*.

Description

An LDAP operations queue is in distress and has exceeded capacity.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1621 – LDAP Queue Cleared

Message

LDAP: Operation queue *{process id}* has cleared and is no longer in distress. Capacity is below *{event msg}*.

Description

An LDAP message that the queue is no longer in distress.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1622 – LDAP Queue Full**Message**

LDAP:Operation queue *{process id}* is currently at 100% and will begin rejecting new LDAP Modify requests.

Description

An LDAP message queue is at 100% capacity and will reject new LDAP modify requests.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1623 – LDAP Modify Fail2**Message**

LDAP: Modify failure. Unable to modify *{fields}* at *{DN}* due to the following error: *{msg}*

Description

Unable to initiate an LDAP modify operation on the specific External Field specified by the user. Example – Modify failure. Unable to modify *External Field Name* at LDAP *DN* due to the following error: *reason*

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1624 – LDAP Modify Fail

Message

LDAP: Modify failure. Unable to perform modify due to the following error: *{msg}*

Description

Unable to initiate an **LDAP** modify operation because the LDAP data source does not support this operation. Example – Modify failure. Unable to perform modify due to the following error: *Data source is not configured with External Fields and will not support this update.*

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1626 – No Configured Data Sources

Message

LDAP:Update unsuccessful: *{msg}*

Description

Unsuccessful LDAP update.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1630 – DHCP Unexpected Event ID Set | Clear**Message**

DHCP: Unexpected problem: *{msg}*

Description

DHCP: Unexpected problem: *0*.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1631 – DHCP Unable To Bind Event ID

Message

DHCP: Unable to bind to port *{port num}* for listening

Description

DHCP is unable to bind to the specified port for listening.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1632 – DHCP Response Timeout Event ID

Message

DHCP: Timeout waiting for response from *{id}*

Description

DHCP timed out waiting for a response from the indicated source.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1633 – Bad Relay Address Event ID Set | Clear**Message**DHCP: Bad relay address *{ip address}***Description**

DHCP: Bad relay address.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1634 – Bad Primary Address Event ID Set | Clear**Message**DHCP:Bad primary address *{ip address}***Description**

DHCP encountered a bad primary address.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1635 – Bad Secondary Address Event ID Set | Clear

Message

DHCP:Bad secondary address *{ip address}*

Description

DHCP encountered a bad secondary address.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1641 – Searching Event ID

Message

{0}: Searching for *{event id}*

Description

Searching for the specified event ID.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. No action required.

1642 – Results Event ID**Message***{msg type}: Result for {ip address}: {cpe mac address}, xid: {agent mac address}***Description**

Results of a search CPE by IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery:

1. No action required.

1661 – EL Bad Realm**Message**SH:Peer Realm *{msg details}***Description**

A bad realm is configured.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1662 – EL Bad Address

Message

SH:Bad *{primary | secondary}* address *{ip address}*

Description

SH bad IP address configured.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1663 – EL Searching

Message

SH: Searching for *{peer id}*: *{subscriber id}*

Description

Started search for subscriber in Diameter Peer HSS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1664 – EL Search Results**Message**SH:Search results for *{stype}* *{filter}* are: *{results}***Description**

Search results for user from Diameter Peer HSS

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1665 – EL No Matches**Message**SH:No matches for *{stype}* *{filter}*

Description

No results found for user from Diameter Peer HSS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1666 – EL Unexpected Search Failure

Message

SH:Unexpected search failure on *{peer id}*

Description

Unexpected SH search failure.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1667 – EL Subscribing

Message

SH: Subscribing for *{key}: {id}*

Description

SH: Subscribing for user profile change notifications for a subscriber.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required.

1668 – EL Subscribe Results

Message

SH: Subscription results for *{key} {id}* are: *{results}*

Description

Subscription results for user from Diameter Peer HSS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1669 – EL Subscribe Fail

Message

SH:Unexpected subscription failure for *{key} {id}*, reason: *{reason}*

Description

SH: Unexpected subscription failure.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1670 – EL Unsubscribing

Message

SH: Unsubscribing for *{key}: {id}*

Description

Unsubscribing for user profile change notifications for a user.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server
MPE

Group
LDAP

Recovery

1. No actions are required

1671 – EL Unsubscribe Results

Message

SH: Unsubscription results for *{key}* *{id}* are: *{results}*

Description

Unsubscription results for user from Diameter Peer HSS.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1672 – EL Unsubscribe Failure

Message

SH:Unexpected unsubscription failure for *{key}* *{id}*, reason: *{reason}*

Description

Unexpected unsubscription failure.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1673 – EL Notification

Message

SH: Received notification: *{results}*

Description

Received a notification.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

LDAP

Recovery

1. No actions are required

1674 - EL Updating

Message

SH: Updating user *{key}*: *{id}* *{results}*

Description

Updating user

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery:

1. No action required.

1675 - EL Update Failure**Message**SH: Update results for *{sub id} {1}* are: *{reason}***Description**

Update for specified subscriber failed for the indicate reason.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. If the problem persists, contact [My Oracle Support](#).

1676 - EL Update Out of Sync**Message**SH:Update Out-Of-Sync for *{sub id} {peer id}***Description**

Update out of sync for specified subscriber ID.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. No action required.

1681 – MSR Connection

Message

MSR: Established connection to *{ip address:port num}*

Description

A new connection to the server at the specified IP address was established.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1682 – MSR Connection Closing

Message

MSR: Closing connection to *{ip address:port num}*

Description

The connection to the server at the specified IP address was closed.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1684 – SPR Connection Closed

Message

MSR: Closing connection to *{ip address:port num}* in order to revert to primary

Description

Closing a secondary MSR connection to revert to a primary connection. Occurs when flipping back from secondary to primary MRA connection.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

MSR

Recovery

1. Self recovery; no action required.

1685 – MSR DB Not Reachable

Message

MSR: Attempted connection to *{ip address:port num}* failed, reason: *{msg}*

Description

Connection attempt to the MSR server at the specified IP address failed for the specified reason.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

MSR

Recovery

1. Verify that there is not a problem with the MSR server or the network path used to reach the server.

1686 – MSR Search

Message

MSR: Searching for *{stype}: {key}*

Description

A search is being performed for the search type using the specified key.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1687 – MSR Search Result**Message**MSR: Search result for *{stype} {key}* is: *{result}***Description**

The results of the search request.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1690 – MSR Search Fail**Message**MSR: Unexpected search failure for *{stype} {key}*, reason: *{msg}***Description**

A search was terminated for the specified unexpected reason.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1691 – MSR Update

Message

MSR: Updating *{type}*: *{key}*

Description

An update is being performed for the update type using the specified key.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1692 – MSR Update Result

Message

MSR: Update results for *{type}* *{key}* are: *{result}*

Description

The results of the update request.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1693 – MSR Update Fail**Message**MSR: Unexpected update failure for *{type}* *{key}*, reason: *{msg}***Description**

An update was terminated for the specified unexpected reason.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1694 – MSR Sub**Message**MSR: Subscribing for *{type: {key}}***Description**

A subscription is being performed for the subscription type using the specified key.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1695 – MSR Sub Result

Message

MSR: Subscription results for *{type}* *{key}* are: *{result}*

Description

The results of the subscription request.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1696 – MSR Sub Fail

Message

MSR:Unexpected subscription failure for *{0}* *{1}*, reason: *{2}*

Description

A subscription was terminated for the specified unexpected reason.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1697 – MSR Unsub**Message**

MSR: Unsubscribing for *{type}: {key}*

Description

An unsubscription is being performed for the subscription type using the specified key.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1698 – MSR Unsub Result

Message

MSR: Unsubscription results for *{type}* *{key}* are: *{result}*

Description

The results of the unsubscription request.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

1699 – MSR Unsub Fail

Message

MSR: Unexpected unsubscription failure for *{type}* *{key}*, reason: *{msg}*

Description

An unsubscription was terminated for the specified unexpected reason.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. Check the cause of the exception and check the MSR configuration for any errors that might have caused the problem.

1711-BRAS Handle DRQ**Message**COPS-PR: Received *{msg type}* from *{gate id}***Description**

The specified message type was received from the specified gateway.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

No actions are required.

1801 – PCMM No PCEF**Message**PCMM:No PCEF available for SubId *{0}***Description**

This trace log records every PCMM request when the MPE cannot find PCEF. The tracelog is disabled by default unless the user sets "RC.TrapNoPcefEnabled" to "true" in RcMgr. This update occurs in both MPE-R and MPE-S. The SubId in the log details is CMTSIP if MPE uses CMTSIP to find PCEF when it receives PCMM requests. The PCMM requests may be GateSet | GateInfo | GateDelete.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

1805 - PCMM No Connection PCEF

Message

PCMM: No connection to PCEF. Host name: *{host name}*

Description

PCMM has no connection to PCEF.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2198 – SMSR SMSC Switched to Primary

Message

SMPP: Switched back to primary SMSC *{ip address | host name}*.

Description

SMPP switched back to the primary SMSC located at the indicated IP address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMPP

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2199 - SMSR SMSC Switched to Secondary**Message**

SMPP: Lost connection to primary SMSC *{ip address | host name}*. Switched to secondary SMSC *{ip address | host name}*.

Description

SMPP lost the connection to the primary SMSC and switched to the secondary SMSC.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMPP

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2210 - Reached Max Gates Event ID | Clear

Message

MGPI:{*ip address*} reached max upstream gates

Description

A subscriber at IP address has reached the configured maximum number of upstream gates.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MGPI

Recovery

1. No action is required.

2211 – Reached Max GPI Event ID Set | Clear

Message

MGPI: {*ip address*} reached max GPI on all upstream gates

Description

A subscriber at IP address has reached the configured maximum grants per interval on all upstream gates.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MGPI

Recovery

1. This subscriber address is exceeding the capacity; attention is required.
2. If the problem persists, contact [My Oracle Support](#).

2212 - Incrementing GPI Event ID**Message**

MGPI: Incrementing GPI for gateid:{*gate id*}, amid:{*am id*}, subscriber:{*sub id*} to {*num*}

Description

The grant per interval for the specified gate, AMID, and subscriber has been increased to num.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MGPI

Recovery

1. No actions required.

2213 – Decrementing GPI Event ID**Message**

MGPI: Decrementing GPI for gateid:{*gate id*}, amid:{*am id*}, subscriber:{*sub id*} to {*num*}

Description

The grant per interval for the specified gate, AMID, and subscriber has been decreased to num.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MGPI

Recovery

1. No action is required.

2300 – Time Period Changed

Message

TOD: Time period(s) changed from *{prev time}* to *{new time}*.

Description

The current time period has changed. (This may not affect any sessions.)

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2301 – Transition Started

Message

TOD: Transition to time period(s) *{0}* started.

Description

A time period transition has started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2302 – Transition Aborted**Message**

TOD: Transition to time period(s) *{new time}* was still in progress when time periods changed. Transition aborted.

Description

A time period transition was started before a previous transition was completed. The time transition was canceled.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2303 – Transition Succeeded**Message**

TOD: Transition to time period(s) *{new time}* successfully completed.

Description

A time period transition has finished and all affected sessions have been updated accordingly.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2304 – Transition Failed

Message

TOD: Transition to time period(s) *{new time}* failed to complete normally.

Description

A time period transition was not completed due to a communication failure with the policy enforcement device.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2305 – Transition Aborted On Demand

Message

TOD: Transition to time period(s) *{new time}* was aborted.

Description

An operator has manually canceled a time period transition.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2306 – Tasks Scheduled On Demand

Message

TOD: Transition to time period(s) *{new time}* was invoked by the operator.

Description

A transition to a time period was invoked by the operator.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Time-of-Day

Recovery

1. No actions are required.

2547 – SMS Delivery Date In Past

Message

SMS: Delivery date lies in past, *{delivery date calculated}*.

Description

"SMS: Delivery date lies in past, expert setting
SendSMSNowWhenDeliveryDateInPast set to false, dropping SMS notification" or
"SMS: Delivery date lies in past, expert setting
SendSMSNowWhenDeliveryDateInPast set to true, sending SMS with immediate
delivery."

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. Configure a delivery date in the user profile that is not in the past.

2548 – SMS Send Global Billing Day

Message

SMS: Billing day not available for user: *{user id}*, considering global billing day *{global billing day}* for delivery date calculations.

Description

This trace log message is displayed when the billing date is configured as '0' in the user profile.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery:

1. Configure a valid billing date within the range of 1 to 31 in the user profile. if a valid billing date is not configured, the global billing date will be used by default as the billing date for delivery date calculations.

2549 – SMSR Queue Full**Message**

SMS: SMSR internal queue is full: *{queue name}*. Messages will be rejected until space becomes available.

Description

SMSR queue has reached capacity. Messages will be rejected until space becomes available.

Severity

Warning

Notification

Trace Log

Alarm

Yes - 72549

Trap

No

Server

MPE

Group

SMS

Recovery

1. No actions are required.

2550 – SMS Not Enabled

Message

SMS: SMS Relay is not enabled to receive message. *{0}*

Description

SMS Relay is not enabled. An Info level entry is logged if the event occurs during reconfiguration. A Warning level entry is logged if the event occurs during operation.

Severity

Info, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. No action is required.

2551 – SMS Config Endpoint

Message

SMS: Configured SMS Relay endpoint: *{host name:port num/path_to_service}*

Description

Configured SMS Relay endpoint.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. No actions are required

2552 – SMS Send Success

Message

SMS: Sent to {0} using SMS Relay defined at {1}# Message:{2}

Description

Sent message using SMS Relay.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. No actions are required

2553 – SMS Billing Day Send Failure

Message

SMS: Unable to send SMS to {user id}. Invalid Delivery Day {delivery date calculated} configured.

Description

This trace log message is triggered when a user configures an invalid delivery date in the policy action such as using 0 or a negative integer. This trace log message is also triggered if a configured smart string does not resolve to a positive integer.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery:

1. Configure a valid billing date in the user profile. Configure the date as a smart string so that it will resolve to a valid day of month.

2554 – SMS Send Delivery Date

Message

SMS: Sending SMS {*SMS content*} to user {*user id*} on Delivery Date {*Calculated delivery date*}

Description

This trace log is triggered when an SMS is sent successfully on the scheduled delivery date. The purpose of this log is to display the date on which an SMS is going to be delivered to the end user.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

No action required.

2555 – SMS Send Error

Message

SMS: Error sending SMS to {*sub id*} using SMS Relay defined at {*ip address*}# Message: {*msg contents*}

Description

An error occurred when sending SMS using defined SMS Relay.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. No actions are required

2556 – SMS Send Failure**Message**SMS: Unable to send SMS to *{sub id}* using SMS Relay defined at *{ip address}***Description**

Unable to send SMS using defined SMS Relay.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. No actions are required

2557 – SMS Failure No MSISDN**Message**SMS: Unable to send SMS to *{sub id}*. User's MSISDN could not be found.

Description

Unable to send SMS because user's MSISDN not found.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMS

Recovery

1. No actions are required.

2558 – SMS Connection Established To SMSC

Message

SMS: Connection established to SMSC *{ip address}*

Description

This trace log is triggered when a connection is established to the SMSC.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMPP

Recovery

1. No actions are required.

2559 – SMSR SMSC Conn Closed

Message

SMS:Connection has been closed to SMSC *{ip address}*

Description

The connection to the SMSC is lost.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMPP

Recovery

1. No actions are required.

2560 – Email Not Enabled Info | Warn

Message

SMTP: SMTP functionality is not enabled to send message. *{0}*

Description

SMTP functionality is not enabled to send message.

Severity

Info, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2561 – Email Config Endpoint

Message

SMTP: Configured endpoint: *{ip address:port num/path/service name}*

Description

The SMTP endpoint was configured.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. No action required.

2562 – Email Send Success

Message

SMTP:Sent to id: *{sub id}* using SMS Relay defined at *{ip address:port num/path/service}#*

Subject:*{msg subj}*

Description

SMTP sent an email successfully to the specified subscriber using the indicated SMS Relay endpoint.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. No action required.

2563 – Email Send Error

Message

SMTP: Error sending SMTP message to *{sub id}* using SMS Relay defined at *{ip address:port num/path/service name}*# Subject: *{msg subj}*# Message: *{msg contents}*

Description

An error occurred while sending an email to the specified subscriber using the indicated SMS Relay endpoint. The email subject and contents are detailed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2564 – Email Send Failure

Message

SMTP: Unable to send SMTP message to *{sub id}* using SMS Relay defined at *{ip address:port num/path/service name}*

Description

Unable to send email using the defined SMS Relay endpoint.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2565 – SMSR SMTP Conn Closed

Message

SMTP: Connection to MTA was closed.

Description

The connection to the MTA was lost.

Severity

Warning

Notification

Trace Log

Alarm

Yes – 72565

Trap

No

Server

MPE

Group

SMTP

Recovery

1. No actions are required.

2566 – SMTP Connection Established | Warn

Message

SMTP: Connection established to MTA *{ip address}*

Description

A connection to the MTA was established.

Severity

Info, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. No actions are required.

2567 – SMTP Connection Error**Message**

SMTP: Error attempting to establish a new connection to *{ip address}*. Error: *{error msg}*

Description

A connection to the specified MTA could not be established.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. No actions are required.

2568 – HTTP Connection Established

Message

Policy Notification: Connection established to server *{URL}*

Description

A connection established from the SMSR to a configured destination.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

HTTP

Recovery

1. No action required.

2569 – HTTP Connection Error | SMSR HTTP Conn Closed

Message

Policy Notification: Error attempting to establish a new connection to *{URL}*.

Policy Notification: Lost connection with destination *{iURL}*

Description

A connection between the SMSR and the configured destination was closed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

HTTP

Recovery

1. Check the network connectivity between SMSR and configured destination.
2. Check configured URL.

2570 – HTTP Queue Clear Size Reached**Message**

Notification queue is at {#}% capacity

Description

Warning to indicate that notifications are backing up because of connection or latency problems.

Severity

Warning

Notification

Trace Log

Alarm

Yes, 72549

Trap

No

Server

MPE

Group

HTTP

Recovery

1. Check the network connectivity between the SMSR and configured destination or check for heavy traffic between the SMSR and configured destination.

2571 – Generic Notification Send Error**Message**

Policy Notification: Error sending Notification to {#}

Message:{#}

Description

An error to indicate that the notification message was unable to be sent from the MPE to the SMSR.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

HTTP

Recovery

1. If the problem persists, contact [My Oracle Support](#).

2611 – MSR Receive Notification

Message

MSR: Received notification: *{msg}*

Description

The specified notification was received from the MSR about a subscriber profile change.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MSR

Recovery

1. No actions are required.

2700 – Binding Created

Message

DRA: Binding Created for subscriber *{sub id}* with server identity *{device name}*

Description

A new **DRA** binding was created and an MRA device was selected for the subscriber's sessions.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2701 – Binding Released**Message**DRA: Binding Released for subscriber *{sub id}* with server identity *{device name}***Description**

A DRA binding was released between the named subscriber and MRA device because the subscriber's last session was terminated.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2702 – Binding Found

Message

DRA: Binding Found for subscriber *{sub id}* with server identity *{device name}*

Description

An existing binding was found (and possibly updated) between the specified subscriber and MRA device.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2703 - Binding Not Found

Message

DRA: Binding NOT found for subscriber *{sub id}*

Description

The MRA device did not find binding information for the named subscriber and has to either query another MRA device or respond to a requesting MRA device.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2704 - Binding Release Task**Message**

DRA: Binding Release Task {*STARTED* | *COMPLETED* | *ABORTED*} Total time : {1}
{2}

Description

A binding release task has either started, completed, or aborted.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2705 – Duplicate Bindings**Message**

DRA: Duplicate bindings have been detected for {*sub id list*} on {*device list*}

Description

Duplicate bindings have been found for the list of subscribers on the list of MRA devices.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2706 – Suspect Cleanup Start

Message

DRA: Binding cleanup task has been started

Description

Indicates that the cleanup task to look for stale sessions and suspect bindings has started or is currently running.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2707 – Suspect Cleanup Finished

Message

DRA: Binding cleanup task is finished and processed *{num}* stale bindings, *{num}* duplicate bindings, and *{num}* stale sessions

Description

Indicates that the cleanup task to look for stale sessions and suspect bindings has finished.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery:

1. No actions are required.

2708 – DRA Cleanup Task Finished Iter**Message**

DRA: Binding Finished iterating the database

Description

Indicates the cleanup task is now finished for its current cycle, and displays the number of stale bindings, duplicate bindings, and stale sessions detected.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

MRA

Recovery

1. No actions are required.

2710 – RADIUS Cleanup | RADIUS Server Stop**Message**

RADIUS: Clean up task finished. Cleaned up *{num}* sessions of *{1}* in *{time}* seconds.
RADIUS: Stopping communication for port *{port num}*

Description

Severity

Info, Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery:

1. No actions are required

2711 – RADIUS Cleanup Failed

Message

RADIUS: Failed to cleanup session *{sess id}* from **BNG** *{ip address}*.

Description

RADIUS failed to cleanup session.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery:

1. No actions are required

2712 – RADIUS Cleanup Started

Message

RADIUS: Clean up task started at *{mm/dd/yy hh:mm AM | PM}*.

Description

The RADIUS cleanup task started at the specified day and time.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. No actions are required

2713 – RADIUS Rejected On TDF Failure | RADIUS Send Failure

Message

RADIUS: Rejecting request *{0}* as TDF *{1}* reported error or timed out.

RADIUS: Failed to send *{0}* / *{1}* [*{2}* / *{3}*] from *{4}* *{5}*

Description

RADIUS rejected a request because TDF reported an error or the request timed out.

RADIUS failed to send the specified message from the specified device.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. No actions are required

2720 – Mapping Cleanup Start

Message

DRA: Mapping cleanup task has been started

Description

The Mapping cleanup task has started.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DRA

Recovery

1. No actions are required

2721 – Mapping Cleanup Finished

Message

DRA: Mapping cleanup task is finished and processed *{num}* stale mappings

Description

The Mapping cleanup task is finished and processed the indicated number of stale mappings.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

DRA

Recovery

1. No actions are required

2900 – ADMISSION Protocol Busy Event**Message**

ADMISSION: System is in busy state : {0}

Description

The current system load is evaluated by an admission controller as exceeding admission criteria thresholds.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Load Admission

Recovery

1. Typically, this condition returns to normal state. If it persists, contact [My Oracle Support](#).

2901 – ADMISSION Protocol Clear Event**Message**

ADMISSION: System is in normal state : {0}

Description

The current system load is below clearing admission criteria thresholds and stability timeout is exceeded.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Load Admission

Recovery

1. No actions are required.

2902 – ADMISSION Component Busy Event

Message

ADMISSION: {3}: Resource {res name} : new condition {1} of the criteria {threshold}

Description

The load of the monitored resource is evaluated by an admission controller as exceeding the admission criteria threshold. This event carries only an informative value and can be disabled by the `ResourceStateLog` property.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Load Admission

Recovery

1. Typically, this condition returns to normal state. If it persists, contact [My Oracle Support](#).

2903 – ADMISSION Component Clear Event

Message

ADMISSION: {3}: Resource {res name} : new condition {1} of the criteria {threshold}

Description

The load of the monitored resource is below the clearing criteria threshold. This event carries only an informative value and can be disabled by the ResourceStateLog property.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE, MRA

Group

Load Admission

Recovery

1. No actions are required.

2904 – Diameter Too Busy Set | Clear

Message

ADMISSION: {0} is in a {1} state

Description

Diameter/RADIUS protocol is in a busy state.

Severity

Warning

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Load Admission

Recovery

1. Self-recoverable when load drops below cleanup threshold; if persisted, identify the source of the high Diameter/RADIUS load.

2905 – RADIUS Too Busy | Clear

Message

ADMISSION: {0} is in a {1} state

Description

Diameter/RADIUS protocol is in a normal state.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Load Admission

Recovery

1. Self-recoverable when load drops below cleanup threshold; if persisted, identify the source of the high Diameter/RADIUS load.

3000 – Trace Log Rate Limit

Message

The trace log has throttled *{num}* messages in the past *{time}* seconds

Description

Messages are throttled when the message rate is above the configured rate of 10 per second (the default value).

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

N/A

Recovery

1. No actions are required.

3100 – Cert Interval Days

Message

Certificate Interval less than or equal to zero. SubjectDN name "{0}". Days: {1}

Description

The SSL certificate specified will expire in 1 days. Note: A 90-day SSL certificate is installed by default when a fresh software installation occurs on a system. The expiration of this certificate can cause this trace log code to be generated.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

Certificate Monitor

Recovery

1. Delete the expiring SSL certificate using the Platform Configuration utility to prevent this warning message from being generated again. Platform Configuration procedures are available in the *Platform Configuration User's Guide*.
2. If using https or encryption between servers, create a new certificate using the Platform Configuration utility.

3101 – Cert Interval

Message

Certificate Interval less than or equal to zero. SubjectDN name "{0}".

Description

The certificate interval is less than or equal to zero.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

Certificate Monitor

Recovery

1. Delete the expired SSL certificate using the Platform Configuration utility to prevent this warning message from being generated again. Platform Configuration procedures are available in the *Platform Configuration User's Guide*.
2. If using https or encryption between servers, create a new certificate using the Platform Configuration utility.

4000 – Policy Critical Alarm | Clear

Message

Critical Action Alarm: {0}, of policy "{name}" with ID - {sub id}

Description

Arbitrary alarm whose cause (and resolution) depends on the policy definition.

Severity

Critical

Notice

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Load Admission

Recovery

1. Recovery is based on each individual case.

4001 – Policy Major Alarm | Clear**Message**

Major Action Alarm: {0}, of policy "{name}" with ID - {sub id}

Description

Arbitrary alarm whose cause (and resolution) depends on the policy definition.

Severity

Error

Notice

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Load Admission

Recovery

1. Recovery is based on each individual case.

4002 – Policy Minor Alarm | Clear**Message**

Minor Action Alarm: {0}, of policy "{name}" with ID - {sub id}

Description

Arbitrary alarm whose cause (and resolution) depends on the policy definition.

Severity

Warning

Notice

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Load Admission

Recovery

1. Recovery is based on each individual case.

4048 – PCMM Unknown GateID

Message

PCMM: Protocol error - unknown gate id. Gate Id: *{gate id}*

Description

A PCMM message was received with a Gate ID that does not correspond to any session in the MPE database.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If the problem persists, contact [My Oracle Support](#).

4063 – NAC Session Context Format Error

Message

CAC: Session context format error for session *{sess id}* - removing

Description

The MPE device encountered a session context format error for the specified session and removed the session.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If the problem persists, contact [My Oracle Support](#).

4069 – CAC Remove Fail**Message**

CAC: Attempt to remove non-existent session ID {0} failed

Description

The VoD server attempted to release a session that no longer exists (or never existed).

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If the problem persists, contact [My Oracle Support](#).

4080 – NAC Session Lookup Fail

Message

CAC: Error locating session in CAC database: *{error msg}*

Description

There was a problem reading the session database.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If problem persists, contact [My Oracle Support](#).

4143 – CAC DB Write Fail

Message

CAC: Exception while writing session database.

Description

This is an internal configuration error.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If problem persists, contact [My Oracle Support](#).

4154 – NAC VOD Server Activate**Message**

NAC: VOD Server Activate.

Description

The VoD server is now active.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If problem persists, contact [My Oracle Support](#).

4155 – NAC VOD Server Deactivate**Message**

NAC:VOD Server Deactivate

Description

The VoD Server is now inactive.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If problem persists, contact [My Oracle Support](#).

4156 – PCMM Unknown

Message

PCMM: Protocol error - unknown. Gate Id: *{gate id}*; Error Code: *{code}*

Description

There was an internal error while releasing resources.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If problem persists, contact [My Oracle Support](#).

4157 – PCMM Protocol Error

Message

PCMM: Protocol error. Gate Id: *{gate id}*

Description

PCMM encountered a protocol error from the specified gate ID.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. If problem persists, contact [My Oracle Support](#).

4208 – CAC Dupe Session Status**Message**

CAC: {0} reserve of duplicate session {1} on {2} complete: status {3}, duration {time}ms

Description

A session with a duplicate ID was successfully reserved.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Recovery

1. No action required.

4300 - RC Conn Lost**Message**

Rc {ip address} Unreachable

Description

The CMP-to-MPE connection has failed.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Load Admission

Recovery

1. Policy execution INFO trace log

4301 - RC Conn Restore

Message

Rc *{ip address}* Reachable

Description

The CMP-to-MPE connection has been restored.

Severity

Info

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

CMP, DC

Group

Load Admission

Recovery

1. Policy execution INFO trace log

4302 – RC Unreachable

Message

Rc *{ip address}* Unreachable - Operation: *{operation}*

Description

The CMP-to-MPE connection failed during the specified operation.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Load Admission

Recovery

1. Policy execution INFO trace log.
2. If the problem persists, contact [My Oracle Support](#).

4303 – RC Log Download Fail**Message**Can not download log file from Rc {*ip address*}**Description**

Cannot download log file from Rc.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

4550 – Policy Info**Message**Policy Trace {0}: {*policy name*}

Description

Policy generated Info level Trace Log notification.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy execution INFO trace log

4551 – Policy Warn

Message

Policy Trace {0}: {policy name}

Description

Policy generated WARNING level Trace Log notification.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy execution WARN trace log

4552 – Policy Debug

Message

Policy Trace {0}: {policy name}

Description

Policy generated Debug level Trace Log notification.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy execution DEBUG trace log

4560 – Policy Trace Action Emergency

Message

Policy Action Trace: {policy notification}

Description

Policy Action generated Emergency Trace Log notification.

Severity

Emergency

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log EMERGENCY action

4561 – Policy Trace Action Alert

Message

Policy Action Trace: *{policy notification}*

Description

Policy Action generated Alert Trace Log notification.

Severity

Alert

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log ALERT action

4562 – Policy Trace Action Critical

Message

Policy Action Trace: *{policy notification}*

Description

Policy Action generated Critical Trace Log notification.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log CRITICAL action

4563 – Policy Trace Action Error**Message**Policy Action Trace: *{policy notification}***Description**

Policy Action generated Error Trace Log notification.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log ERROR action

4564 – Policy Trace Action Warning**Message**Policy Action Trace: *{policy notification}***Description**

Policy Action generated Warning Trace Log notification.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log WARNING action

4565 – Policy Trace Action Notice

Message

Policy Action Trace: *{policy notification}*

Description

Policy Action generated Notice Trace Log notification.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log NOTICE action

4566 – Policy Trace Action Info

Message

Policy Action Trace: *{policy notification}*

Description

Policy Action generated Info Trace Log notification.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log INFO action

4567 – Policy Trace Action Debug**Message**Policy Action Trace: *{policy notification}***Description**

Policy Action generated Debug Trace Log notification.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Load Admission

Recovery

1. Policy generated trace log DEBUG action

4600 – Secondary Connection Rejected**Message**

A Secondary connection from *{ip address}* has been rejected because a Primary connection is already established.

Description

A Secondary connection has been rejected due to a Primary connection already existing from the same Diameter identity. This could indicate a split brain situation at the remote identity.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Georedundancy

Recovery

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. If alarm persists, contact [My Oracle Support](#).

4601 – Secondary Connection Reverted

Message

A Secondary connection from *{ip address}* has been disconnected because a Primary connection has been established.

Description

A connection has reverted from a Secondary connection to a Primary connection. While this could happen normally during a remote failover, it could also indicate a potential split brain situation at the remote cluster.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE, MRA

Group

Georedundancy

Recovery

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. If alarm persists, contact [My Oracle Support](#).

4610 – SH Connection OPT**Message***{0} # {1}***Description**

The CMP server performed a global operation to enable (or disable) Sh on all MPE devices with the results specified (MPE devices for which it was successful are listed; MPE devices for which the operation failed are also listed).

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

SH

Recovery

1. If the operations failed for some MPE devices then it can be retried. If repeated attempts fail then there may be other management issues with the associated MPE devices and connectivity to those devices should be verified.

4700 – UME CMD Return Msg**Message**Upgrade Manager: execute command *{cmd}* *{msg}***Description**

Upgrade Manager executes command on remote server and gets the return message, then generates the Info Trace Log notification.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

Upgrade

Recovery

1. No action required.

4701 – Diam Msg Send Failed

Message

Diameter: Unable to send msg as peer seems to be disconnected: *{peer id}*

Description

Diameter unable to send message because peer node seems to be disconnected.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

Upgrade

Recovery

1. No action required.

6000 – Sync Log | Wireline Subact Log

Message

{log}

Description

The log describes the subscriber account information which can be associated to the VoD reserve, release, etc.

Severity

Emergency

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MPE

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6001 – Subact Log | Wireline Sync Log

Message

{0}

{1}

{log}

Description

The log describes the synchronized information of the synchronization sessions.

Severity

Emergency

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

MPE

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6102 – State Sync Mgr Endpoint

Message

Gx-Plus: Learnt new endpoint *{ip address}*, *{sess id}* from gateway *{gw ip address}*

Description

The PCRF has learned a new subscriber endpoint with the specified session ID from the gateway. The *gw ip address* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE diameter identity is returned.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1756

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6103 – VOD Terminate CAC Session

Message

VOD: Terminate CAC Session. Server Type: *{0}*; Ip: *{ip address}*; Id: *{id}*

Description

This is an internal configuration error.

Note: Supersedes event 4068.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4201

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6105 – PCMM XML Syntax Error**Message**Incorrect XML syntax in PCMM services file *{error msg}#{file name}***Description**

BoD received an error message from file name.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6200 – NAC Abnormal Session Delete**Message**NAC: Abnormal delete of session. *{sess id}*, Reason Code: *{code}*, Text: *{msg}*.

Description

Session deleted abnormally. An element-level statistic in the MPE device tracks total normal disconnects per network element. The CMP server retrieves this statistic as part of the current call for network element statistics using the OM Stats Task.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

NAC

Deprecated ID

1314

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6201 – NAC Normal Session Delete

Message

NAC: Normal delete of session. *{sess detail}*.

Description

The session is deleted normally. The *sess detail* includes the Subscriber ID, the format of which changes depending on whether the subscriber has a dynamic or static IP address (static IP subscribers do not have the @BRAS on their ID). An element-level stat in the MPE device tracks total normal disconnects per network element. The CMP server retrieves this stat as part of the current call for network element stats using the OM Stats Task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server
MPE

Group
NAC

Deprecated ID
1315

Recovery

1. No action required.

6202 – NAC Allow Session

Message
NAC: Allowed session. *{sess detail}*.

Description
The MPE device allowed the session. Upon completion of each session request (blocked or allowed) from the VoD server, the MPE device generates an Info level event log. The following data is provided within the message: reason code (if applicable), account id, subscriber data, network element name, and full network path.

Severity
Info

Notification
Trace Log

Alarm
No

Trap
No

Server
MPE

Group
NAC

Deprecated ID
1316

Recovery

1. No action required.

6203 – NAC Reject No Path

Message
NAC: Rejecting *{msg type}* - no path available from *{sub ip address}* to *{server ip address}*

Description

A request was received but there was no provisioned path that could be used to satisfy the endpoints in the request.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

NAC

Deprecated ID

1320

Recovery

1. Check the specified subscriber IP address and Server IP address and determine if there is a path that should be used.
2. If such a path exists, make sure that the B-RAS in the path is actually associated with the MPE device in the CMP server.

6204 – NAC Reject Sub

Message

NAC: Rejecting *{msg type}* - subscriber with address *{sub ip address}* is unknown (session ID *{vod id}*)

Description

A subscriber without an associated account requested a VoD session. The session request was denied.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server
MPE

Group
NAC

Deprecated ID
1321

Recovery

1. Check to make sure that there is an account for the specified subscriber in the OSS.
2. Make sure that the name of the network element in the account is a B-RAS that is associated with the MPE device in the CMP server.

6205 – NAC Allow Sub

Message
NAC: Allowing *{msg type}* - subscriber with unknown address *{sub ip address}* (session ID *{vod id}*)

Description
A subscriber without an associated account requested a VoD session. The session request was allowed.

Severity
Warning

Notification
Trace Log

Alarm
Yes

Trap
No

Server
MPE

Group
NAC

Deprecated ID
1322

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6206 – NAC Missing Sub Account

Message
NAC: No account information for subscriber *{sub ip address}* (session ID *{vod id}*)

Description

A subscriber with dynamic IP address and without an associated account requested a VoD session. The session request was denied.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

NAC

Deprecated ID

1323

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6207 – NAC Unknown Sub

Message

NAC: Subscriber with address *{sub ip address}* is unknown (session ID *{vod id}*)

Description

A subscriber with an unknown IP address requested a VoD session. The subscriber does not have a static IP address assigned to it, and the subscriber's associated BRAS has not notified the MPE that it has attached to the network.

Note: If event 1324 is generated, either event 1321 or 1322 is also generated.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server
MPE

Group
NAC

Deprecated ID
1324

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6208 – NAC Policy Reject

Message

NAC: Rejecting *{msg type}* - Rejected by policy "{name}"

Description

The specified message was rejected by the specified policy rule.

Note: The MPE device returns a numeric code specified as part of a reject action to the VoD server. The reject code is configured on the CMP server when a Policy is defined. This is available in the GUI as an additional action in the Policy definition dialog. The code itself must be an integer between 0-65535.

Severity
Warning

Notification
Trace Log

Alarm
Yes

Trap
No

Server
MPE

Group
NAC

Deprecated ID
1350

Recovery

1. Check the policy rule and the contents of the message to make sure it is operating as expected.
2. It may be helpful to increase the logging level of the policy log and then repeat this request to examine the details of the policy execution.

6209 – NAC Static Dynamic Defn

Message

NAC: Both static and dynamic definitions for subscriber IP address *{sub ip address}*, using *{dynamic}* definition

Description

In making a video request, a subscriber added a static IP address to an account, but the BRAS to which the subscriber is connected also assigned it a dynamic IP address.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

NAC

Deprecated ID

1351

Recovery

1. Either remove the static IP definition or configure the subscriber on the BRAS to have a static IP address.

6210 – NAC Reject No Endpoint

Message

NAC: Could not find BRAS endpoint *{endpoint}* in path *{path}* - rejecting

Description

An IP subnet pool is improperly associated with a network element (for example, subnet 10.1.x.x is associated with NE1, but NE2 has assigned a subscriber in the same range.)

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

NAC

Deprecated ID:

1352

Recovery

1. Ensure that the IP subnet ranges do not overlap on the network elements.

6211 – IP Already Static**Message**

COPS-PR: Declared an IP address (*{ip address}*) already defined as static in account *{account id}*

Description

A subscriber attached to the network with a static IP address but the BRAS to which the subscriber is connected also assigned a dynamic IP address.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

BRAS

Deprecated ID

1370

Recovery

1. Either remove the static IP definition or configure the subscriber on the BRAS to have a static IP address.

6400 – BRAS Extension

Message

BRAS: Extension - Remote Address: *{ip address}*; old size: *{x}*; new size: *{y}*

Description

The transmit buffer has extended from *x* to *y*. The *ip address* refers to the remote ERX's IP address learned from the COPS socket connection.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

BRAS

Deprecated ID

1740

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6401 – BRAS Contraction

Message

BRAS: Contraction - Remote Address: *{ip address}*; old size: *{x}*; new size: *{y}*

Description

The transmit buffer has decreased from *x* to *y*. The *ip address* refers to the ERX's IP address learned from COPS socket connection.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group
BRAS

Deprecated ID
1741

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6402 – BRAS Overflow

Message

BRAS: Overflow. Remote address: *{ip address}*; needed: *{x}*; remaining: *{y}*

Description

The transmit buffer size for the remote endpoint at IP address needed *x* bytes but only had *y* bytes available.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

BRAS

Deprecated ID

1742

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6403 – COPS Connection Accepted

Message

COPS-PR: Connection accepted from gateway IP:*{ip address}*, port:*{port num}*

Description

A new COPS-PR connection was accepted from the specified gateway. The *ip-address* refers to the remote ERX's IP address learned from the COPS socket connection, and *port num* refers to the port number.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1701

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6404 – BRAS Connection Closed | Clear

Message

COPS-PR: Lost connection with gateway {*gw id*}

Description

The MPE device lost a connection from the gateway. The *gw id* refers to the remote ERX's IP address learned from the COPS socket connection.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1702

Recovery

1. Check availability of the gateway.
2. If the gateway has not failed, make sure the path from the gateway to the MPE is operational.

6405 – COPS Unknown Gateway | Clear

Message

COPS-PR: Rejecting OPN message from *{ip address}*. Unknown gateway

Description

An unknown gateway is trying to establish a COPS-PR connection to the MPE device. The *ip address* refers to the remote ERX's IP address learned from the COPS socket connection, if it's retrieved. Otherwise, "unknown address" is returned.

Severity

Error

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1703

Recovery

1. Check the configuration of the network elements in the CMP server. There should be a B-RAS network element for this gateway and that B-RAS must be associated with this MPE device.
2. Make sure that the configuration of the B-RAS network element is consistent with the provisioned information on the gateway. The network element name in the CMP server must match the provisioned router name on the gateway.

6406 – BRAS Conn Closed

Message

COPS-PR: BRAS IP:*{ip address}*, port:*{num}* no longer associated with this MPE.
Closing connection

Description

BRAS is no longer connected with this MPE device and the connection is being closed.

Severity

Info

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1704

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6407 – BRAS Handle OPN

Message

COPS-PR: Received *{msg type}* from *{gw id}*

Description

The specified message type was received from the specified gateway. The *gw id* refers to the remote ERX's IP address learned from the COPS socket connection.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1711

Recovery

1. No action required.

6408 – BRAS Send Dec Debug

Message

BRAS: Send DEC. DEC: *{msg type}*; Remote address: *{gw id}*

Description

The specified message type was sent to the specified gateway. The *gw id* refers the ERX's IP address learned from COPS socket connection.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1712

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6409 – BRAS Send SSQ

Message

BRAS: Send SSQ. Remote address: *{gw ip}*

Description

The MPE is starting full state synchronization with the specified gateway.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1713

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6410 – BRAS State Sync Complete

Message

BRAS: State sync complete. Remote address: *{gw ip}*

Description

The MPE synchronization with the specified gateway has completed

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1714

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6411 – BRAS Endpoint

Message

BRAS: Endpoint - Ip Addr: *{ip address}*; Sub Id: *{sub id}*; Router Addr: *{ip address}*

Description

The MPE has learned a new endpoint from the specified gateway.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1715

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6412 – BRAS Handle DRQ Msg**Message**

BRAS: DRQ Message - Sub Ip Addr: *{sub ip address}*; Sub Id: *{sub id}*; Router Addr: *{gw ip}*

Description

The MPE device deleted the endpoint *sub ip addresss, sub-id* after the ERX device at *gw ip* sent a DRQ message.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1716

Recovery

1. No action required.

6413 – NAC Stale BRAS Endpoint

Message

NAC: Stale BRAS Endpoint. Ip: *{ip address}*; Sub Id: *{sub id}*; BRAS Addr: *{gw ip}*

Description

The MPE device deleted an endpoint *ip address, sub id* as stale.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1717

Recovery

1. No action required.

6414 – BRAS Send DEC

Message

COPS-PR: Send DEC. Gw name: *{gw ip}*; Local addr: *{mpe ip}*

Description

The ERX *gw ip* requests fast synchronization with Policy Server *mpe ip*.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server
MPE

Group
COPS-PR

Deprecated ID
1722

Recovery

1. No action required.

6415 – Update Session

Message

Handling update. Session Id: *{sess id}*; Subscriber Id: *{sub id}* Router Address: *{gw ip}*

Description

The MPE device received a credit control request for an initial request (CCR-I) with session ID *sess id* and subscriber *sub id* from the gateway *gw ip*. The *gw ip* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is returned.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1750

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6416 – Handle Delete

Message

Handling delete. Session Id: *{sess id}*; Router Address: *{gw ip}*

Description

The gateway *gw ip* sends a CCR-T with a session ID to indicate that a subscriber has logged out and its subscriber data should no longer be associated with an IP address. The *gw ip* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is returned.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1751

Recovery

1. No action required.

6417 – Handle Ack

Message

Handling ack. Endpoint Ip: *{ip address}*; Gx Subscriber Id: *{sub id}*; Router Address: *{gw ip}*

Description

The PCRF has learned of a new subscriber endpoint with *ip address* and subscriber *sub id* from the gateway *gw ip*.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group
Gx-Plus

Deprecated ID
1756

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6418 – State Sync Mgr Sync Start

Message

Gx-Plus: Start state synchronization with gateway {*gw ip*}

Description

The gateway *gw ip* starts a state synchronization with the MPE device. The *gw ip* refers to the GX-MX's Host Name/IP Address configured in the GUI Network Elements tab, if it's set. Otherwise, it's empty.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1763

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6419 – State Sync Mgr Gateway

Message

Gx-Plus: State synchronization with gateway {*gw ip*} has completed

Description

This event signals the completion of state synchronization between the gateway *gw ip* and the MPE device. The *gw ip* refers to the Gx-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is returned.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1764

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6420 – State Sync Mgr Cold Reboot

Message

Gx-Plus: Drop all the bras endpoints and diameter sessions because of cold reboot from gateway {*gw ip*}

Description

When the MPE device receives a JSER from the GWR indicating a cold boot event, it purges all the sessions that were created by requests from the gateway *gw ip*. The *gw ip* refers to the GX-MX's Host Name/IP Address configured in the GUI Network Elements tab, if it's set. Otherwise, it's empty.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1765

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6421 – Handle Delete Subscriber**Message**

Handling delete. Endpoint Ip: *{ip address}*; Gx Subscriber Id: *{sub id}*; Router Address: *{gw ip}*

Description

This event is generated when an endpoint is deleted from the MPE database upon successfully processing a CCR-T message from the gateway *gw ip*. The *gw ip* refers to the remote GX-MX's IP address learned from the diameter socket connection, if the diameter connection exists. Otherwise, the GX-MX's NE Diameter Identity is returned.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1766

Recovery

1. No action required.

6422 – State Sync Mgr Delete Stale**Message**

Gx-Plus: Deleting stale entry for IP *{ip address},{1}* from gateway *{gw ip}*

Description

Once the state synchronization is complete or upon receiving a discovery request, the MPE device performs a scrub operation, by which it deletes all the subscriber information for the gateway *gw ip*, which was not reported by the gateway in the

JSDA messages. This removes stale entries from the MPE databases. The *gw ip* refers to the GX-MX's IP address the from the session logon.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1767

Recovery

1. No action required.

6423 – State Sync Mgr Warn Reboot

MessageGx-Plus: Received warm reboot message from gateway {*gw ip*}**Description**

When the gateway is warm-booted, the gateway *gw ip* sends a JSER to indicate a warm boot event. The *gw ip* refers to the Gx-MX's Host Name/IP Address configured in the GUI Network Elements tab, if it's set. Otherwise it's empty

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1768

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6424 – State Sync Mgr AYT**Message**Gx-Plus: Received AYT message from gateway {*gw ip*}**Description**

The AYT (are you there) event is a ping request from the gateway for the state synchronization application.

This event occurs when the router received no response from the MPE device. This can be caused by a broken connection, a MPE device failover, or a router cold boot. The appearance of this event implies the connection between the router and the MPE device has been recovered. The *gw ip* refers to the GX-MX's Host Name / IP Address configured in the Network Elements tab, if it is set. Otherwise, it is empty.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID

1769

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6425 – State Sync Mgr AWD**Message**Gx-Plus: Received AWD message from gateway {*gw ip*}**Description**

This is the application watchdog event generated by the gateway *gw ip* for the state synchronization application. The *gw ip* refers to the GX-MX's Host Name/IP Address configured in the GUI Network Elements tab if it's set. Otherwise, it's empty.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Gx-Plus

Deprecated ID:

1770

Recovery

1. No action required.

6426 – BRAS Drop

Message

COPS-PR: Dropping *{msg type}* from *{gw ip}* - *{reason}*

Description

There was a protocol error while processing the specified COPS-PR message from the specified gateway. The *reason* provides a more detailed description of the specific protocol error that occurred.

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

COPS-PR

Deprecated ID

1721

Recovery

1. If the problem persists, contact [My Oracle Support](#).

6427 – BRAS Scrubber Logout**Message**

BRAS: Scrubber logout - Ip Addr: *{sub ip address}*; Sub Id: *{sub id}*; Router Addr: *{ip address}*

Description

BRAS Scrubber Logout.

Severity

Info

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE

Group

COPS-PR

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7001 – CAC Session Create Error**Message**

CAC: Exception while recreating Tandberg session.

Description

An exception occurred in a VoD server.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4003

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7002 – CAC Sync Session Recreate

Message

CAC: Recreating Tandberg session *{sess id}* due to sync operation with *{url}*.

Description

Session is being recreated because of synchronization operation with *url*.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4004

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7003 – CAC Session Recreate Fail

Message

CAC: Failed to recreate Tandberg session *{sd}* due to sync with *{url}*: code = *{code}*, desc = *{description}*

Description

Failed to recreate Tandberg session *sess id* due to synchronization with *url*.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4005

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7010 – CAC Session ID List Read Error**Message**

CAC: Exception while reading local session ID list.

Description

This is an internal configuration error.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4065

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7011 – CAC Session Create Fail

Message

CAC: Failed to create CAC session ID *{sess id}*

Description

Could not create CAC Session ID.

Note: Superseded by event 4200.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4066

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7013 – CAC Sync Error2

Message

CAC: Exception while sync operation terminated CAC session ID *{sess id}*.

Description

This is an internal configuration error.

Note: Superseded by event 4201.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4068

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7014 – CAC Remove Session Failed**Message**CAC: Attempt to remove non-existent session ID *{sess id}* failed**Description**

The VoD server attempted to release a session that no longer exists (or never existed).

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4069

Recovery

1. If problem persists, contact [My Oracle Support](#).

7015 – CAC Resource Release Fail**Message**CAC: Failed to release resources for session ID *{sess id}*

Description

A gate could not be set from a rejected reserve request.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4070

Recovery

1. If problem persists, contact [My Oracle Support](#).

7019 – CAC Session Create

Message

CAC: Created CAC session ID *{sess id}* due to request from VoD server at *{ip address}*

Description

The session ID was created successfully.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4096

Recovery

1. No action required.

7023 – NAC VOD Server Sync**Message**

NAC: VOD Server Synchronization.

Description

The VOD server is synchronized.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4110

Recovery

1. No action required.

7025 – NAC Handle Error**Message**

NAC: Handle Error. Code: *{code}*; Subcode: *{subcode}*

Description

The MPE device received a VoD request, but the subscriber IP address cannot be found in the COPS-PR table

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4113

Recovery

1. Check your network configuration.

7027 – NAC Send Error Reply

Message

NAC: Send error reply. Session. *{sess id}*.

Description

This is an internal configuration error.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4115

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7031 – Exception Writing Session

Message

CAC: Exception while writing session database

Description

This is an internal configuration error.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4143

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7032 – CAC Resource Error**Message**CAC: Exception while reserving resources for *{id}*: *{error msg}***Description**

This is an internal configuration error.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4144

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7034 – CAC Session Remove Sync Mismatch

Message

CAC: Locally removing session *{sess id}* due to synchronization mismatch with *{Seachange | Tandberg}* server at *{ip address}*

Description

The CAC AM has a session that is not on the VoD server. As a result, the session is removed and all associated resources are released.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4172

Recovery

1. No action required.

7035 – CAC Session Remove Sync Timeout

Message

CAC: Locally removing session *{sess id}* due to synchronization timeout with *{Seachange | Tandberg}* server at *{ip address}*

Description

Specified session removed due to a synchronization timeout with server with the given IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4173

Recovery

1. No action required.

7036 – CAC Sync Mismatch Session Removal**Message**

CAC: Requesting removal of session *{sess id}* from *{Seachange | Tandberg}* server at *{ip address}* due to synchronization mismatch

Description

Requesting removal of the specified session due to a synchronization mismatch with server with the given IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4175

Recovery

1. No action required.

7038 – NAC VOD Synchronizer Activate**Message**

CAC: This blade is now active

Description

This server is active.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4154

Recovery

1. No action required.

7039 – NAC VOD Synchronizer Deactivate

Message

CAC: This blade is now inactive. Canceling any synchronization in progress.

Description

Indicates the primary server has failed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4155

Recovery

1. Failover to secondary server.
2. If problem persists, contact [My Oracle Support](#).

7047 – CAC Sync Start**Message**

CAC: Starting synchronization with *{ip address}*

Description

Synchronization is started between the MPE device and a VoD server.

Note: Superseded by event 4205.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4164

Recovery

1. No action required.

7048 – CAC Sync End**Message**

CAC: Synchronization with *{0}* complete. Status = *{True | False}*

Description

Synchronization is complete. If Status is True, the synchronization completed successfully. If Status is False, the synchronization was aborted after 20 minutes of retries.

Note: Superseded by event 4206.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4165

Recovery

1. If synchronization continues to fail, contact [My Oracle Support](#).

7052 – CAC Resource Reserve Fail

Message

CAC: Failed to reserve resources for *{sess id}*

Description

The request for resources for the session were denied.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4169

Recovery

1. If problem persists, contact [My Oracle Support](#).

7054 – CAC Dupe Session

Message

CAC: Rejecting create of session ID *{sess id}* from server at *{ip address}*: duplicate session

Description

The creation of the specified session ID was rejected because of a duplicate session.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4177

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7055 – CAC Session Missing

Message

CAC: Tandberg session ID *{sess id}* missing in session list on Tandberg server. Issuing specific query to *{ip address}*

Description

Tandberg session ID missing in session list on Tandberg server. Issuing specific query to *url*.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4178

Recovery

1. No action required.

7056 – CAC Session Missing Remove

Message

CAC: Tandberg Session ID *{sess id}* still missing on Tandberg server at *{ip address}* - scheduling removal

Description

Tandberg session ID *id* still missing in session list on Tandberg server at *url* – scheduling removal.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4179

Recovery

1. No action required.

7057 – CAC Keep Alive Request

Message

CAC: Keepalive status request from Tandberg server at *{ip address}*

Description

Keep alive status request from Tandberg server at the specified IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4180

Recovery

1. No action required.

7058 – CAC Session List Status

Message

CAC: Session list status request from {Seachange | Tandberg} server at {ip address}

Description

Session list status request from indicated server at *ip-address*.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4181

Recovery

1. No action required.

7059 – CAC Session Detail Status

Message

CAC: Session detail status request from Tandberg server at *{ip address}* for session ID *{sess id}*

Description

Session detail status request from Tandberg server at the specified IP address for the session ID.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4182

Recovery

1. No action required.

7060 – CAC Version Status Report

Message

CAC: Version status request from Tandberg server at *{ip address}*

Description

Version status request from Tandberg server at the specified IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4183

Recovery

1. No action required.

7061 – CAC Reserve Session Status**Message**

CAC: {Seachange | Tandberg} reserve of session {sess id} on {ip address} complete: status {status}, duration {time}ms

Description

A session was successfully reserved.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4184

Recovery

1. No action required.

7062 – CAC Session Release Status**Message**

CAC: {Seachange | Tandberg} release of session {sess id} complete: status {status}, duration {time}ms

Description

A session was successfully released.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4185

Recovery

1. No action required.

7063 – CAC Keep Alive No Response

Message

CAC: No keepalive response from Tandberg server at *{ip address}*

Description

No keepalive response from Tandberg server at the specified IP address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4188

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7064 – CAC Session Release Error**Message**

CAC: Exception while releasing session *{sess id}* from Tandberg server

Description

Exception occurred while releasing the specified session id from Tandberg server.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4189

Recovery

1. No action required.

7065 – CAC Session Release**Message**

CAC: Tandberg server requesting release of session ID *{sess id}*: Code = *{code}*, Text = *{description}*

Description

Tandberg server requesting release of session ID with indicated code and description.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4190

Recovery

1. No action required.

7066 – CAC Version Status

Message

CAC: No version status response from Tandberg server at *{ip address}*

Description

No version status response from Tandberg server

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4191

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7067 – CAC Version Report

Message

CAC: Version report from Tandberg server at *{ip address}*: software: *{sw ver}*, interface: *{int ver}*

Description

Software and interface version report from Tandberg server at the specified IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4192

Recovery

1. No action required.

7068 – CAC Invalid Version Report

Message

CAC: Invalid version report from Tandberg server at *{ip address}*

Description

Invalid version report from Tandberg server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4193

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7069 – CAC Keep Alive Send

Message

CAC: Sending keepalive request to Tandberg server at *{ip address}*

Description

Sending keepalive request to Tandberg server.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4194

Recovery

1. No action required.

7070 – CAC Keep Alive Response

Message

CAC: Received keepalive response from Tandberg server at *{ip address}*, code = *{code}*, text = *{description}*, duration *{time}*ms

Description

Received a keepalive response from a Tandberg server with a status of *code* and a status *description*.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4195

Recovery

1. No action required.

7071 – CAC Sync Mismatch**Message**

CAC: Sync mismatch with *{Seachange | Tandberg}* server at *{ip address}*: VoD server has *{num}* sessions missing on MPE

Description

Synchronization mismatch with indicated server at *ip-address*: VoD server has *num* sessions missing on MPE device.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4196

Recovery

1. No action required.

7072 – CAC Sync Mismatch VOD

Message

CAC: Sync mismatch with *{Seachange | Tandberg}* server at *{ip address}*: MPE has *{num}* session *{sess id}* missing on VoD server

Description

Synchronization mismatch with indicated server: MPE device has *num* session *sess id* missing on VoD server.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4197

Recovery

1. No action required.

7073 – Invalid Bit Rate

Message

VOD: Invalid bit rate. Session Id: *{sess id}*; Reservation Client: *{ip address}*; Bit Rate: *{bit rate}*

Description

Session *sess id* from *ip address* was rejected due to invalid bit rate (*bit-rate*)

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group
CAC

Deprecated ID
4198

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7075 – CAC Session Create VOD Fail

Message

CAC: Failed to create CAC session ID *{sess id}* from VoD Server at *{server ip}* for subscriber IP *{sub ip}*: *{status}*

Description

Could not create CAC session ID.

Note: Supersedes event 4066.

Severity
Error

Notification
Trace Log

Alarm
No

Trap
No

Server
MPE

Group
CAC

Deprecated ID
4200

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7076 – CAC Sync Error

Message

CAC: Exception while *{Seachange | Tandberg}* sync operation with *{ip address}* terminated CAC session ID *{sess id}*

Description

This is an internal configuration error.

Note: Supersedes event 4068.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4201

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7078 – CAC Session List Error

Message

CAC: Error requesting session list from *{Seachange | Tandberg}* server at *{ip address}*

Description

This is an internal configuration error.

Note: Supersedes event 4159.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group
CAC

Deprecated ID
4203

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7079 – VOD Sync Now

Message

CAC: Forcing synchronization with *{Seachange | Tandberg}* server at *{ip address}*
VOD: Sync Now. Type: *{Seachange | Tandberg}* URL: *{ip address}*

Description

A manual synchronization has been initiated by a user using the CMP server.

Note: Supersedes event 4163.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4204

Recovery

1. No action required.

7080 – CAC Sync Start Server

Message

CAC: Starting synchronization with *{Seachange | Tandberg}* server at *{ip address}*

Description

Synchronization has started between the MPE device and a VoD server.

Note: Supersedes event 4164.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4205

Recovery

1. No action required.

7081 – CAC Sync Status

Message

CAC: Synchronization with *{Seachange | Tandberg}* server at *{ip address}* complete.
Status = *{True | False}*

Description

Synchronization is complete. If Status is True, the synchronization completed successfully. If Status is False, the synchronization is aborted after 20 minutes of retries.

Note: Supersedes event 4165.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server
MPE

Group
CAC

Deprecated ID
4206

Recovery

1. If synchronization continues to fail, contact [My Oracle Support](#).

7082 – CAC Max Sync Fail

Message

CAC: Max sync failures with *{Seachange | Tandberg}* server at *{ip address}*: removing *{num}* session *{3}*

Description

Synchronization timed out; *num* sessions were removed from the indicated server at the indicated IP address.

Severity
Info

Notification
Trace Log

Alarm
No

Trap
No

Server
MPE

Group
CAC

Deprecated ID
4207

Recovery

1. No action required.

7083 – CAC Dupe Session Status Info

Message

CAC: *{Seachange | Tandberg}* reserve of duplicate session *{sess id}* on *{ip address}* complete: status *{status}*, duration *{time}*ms

Description

A session with a duplicate ID was successfully reserved.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4208

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7084 – CAC Sync VOD Session

Message

CAC: Sync with *{Seachange | Tandberg}* server at *{ip address}*: VoD server has *{num}* session *{sess id}*

Description

Synchronization of VoD session occurred with the indicated server at the specified IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4209

Recovery

1. If the problem persists, contact [My Oracle Support](#).

7085 - CAC Sync Session**Message**

CAC: Sync with {Seachange | Tandberg} server at {ip address}: MPE has {num} session {3}

Description

Occurs when MPE and VOD begin sync. Specifies the current number of local sessions on the MPE, and lists the VOD server's IP address.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

CAC

Deprecated ID

4210

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8001 – BoD Initial Event Log**Message**

Inited EventLog

Description

Initial event log.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8020 – BoD Missing Params HTTP

Message

Invalid HTTP request: missing required arg(s): *{arguments}*

Description

Invalid HTTP request: missing required arguments.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8021 – BoD Failure HTTP

Message

HTTP request failed: *{0}#{1}*

Description

This trace log records failed HTTP requests in BoD. If the value of the CMTSIP that is passed in does not pass the validation of HTTP APIs, then BoD records "Invalid CMTS IP address format encountered (CMTSIP)" in this trace log.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8022 – BoD Unknown SVC Name HTTP**Message**Invalid HTTP request: unknown SERVICENAME: *{svc name}***Description**

Invalid HTTP request: unknown service name.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8023 – BoD Expected Params HTTP**Message**Invalid HTTP request: expected parameters for SERVICENAME *{svc name}*: *{params}*

Description

Invalid HTTP request: expected parameters for service name.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8024 - BoD Classifier Already Active HTTP

Message

Classifier already active for *{sub ip}* - request ignored.

Description

Classifier already active for *subscriber's IP* - request ignored.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8025 - BoD Classifier Not Active HTTP

Message

Classifier not active for *{sub ip}*; - request ignored.

Description

Classifier not active for: *subscriber's IP address* - request ignored.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8050 - BoD Success HTTP

Message

HTTP request success: *{0}*

Description

HTTP request success: *{0}*.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8070 – BoD Failure SOAP

Message

SOAP request failure: *{cmts ip}*

Description

This trace log records failed SOAP requests in BoD. If the value of CMTSIP that is passed in does not pass the validation of SOAP APIs, BoD records “Invalid CMTS IP address format encountered (CMTSIP)” in this trace log.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Deprecated ID

70

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8080 - BoD Success SOAP

Message

SOAP request success: *{ip address}*

Description

SOAP request success.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8100 - BoD Establish Connection PS**Message**Established policy server connection to *{ip address}***Description**Established connection to *server ip address*.**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8102 – BOD Retry Connection PS**Message**Retry reconnect to policy server *{ip address}*; retry attempt *{num}***Description**

Attempt is made to reconnect to policy server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8103 - BOD Drop Connection PS

Message

Policy server connection dropped from *{ip address}*. BoD has scheduled policy server reconnect task.

Description

Once a Policy server is not connected or the connection is broken for some reason, the BoD server will try to re-connect to the Policy server every 1 or 2 seconds and log a Warning message that the corresponding server is disconnected until the Policy server is connected again.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. Restart or reboot the failed MPE device via the CMP server GUI, and make sure the MPE device is online to provide service.

8104 - BoD Disconnect Connection PS

Message

Disconnected policy server connection *{ip address}*

Description

Disconnected Policy Server connection at the specified IP address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8105 - BoD Disconnect Connection Failure PS

Message

Disconnection failure from policy server *{ip address}*

Description

Disconnection failure from policy server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8106 - BoD Establish Connection Failure PS

Message

Could not establish policy server connection to *{ip address}*

Description

Could not establish a policy server connection.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8200 - BoD Change Event Log Level

Message

BoD Event log level changed to: *{new level}*

Description

Change trace log level. Available levels are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice

- Info - default

- Debug

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8250 – BoD Start Session Cleanup Task

Message

BoD session cleanup task starts.

Description

BoD session cleanup task starts.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8251 – BoD Complete Session Cleanup Task

Message

BoD has completed session cleanup task. *{num}* stale sessions have been deleted. It is recommended you perform a database backup before the next auto-delete occurs.

Description

BoD has completed session cleanup task. The number of stale sessions have been deleted. It is recommended you perform a database backup before the next auto-delete occurs.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8252 – BoD Database Backup Failed

Message

BoD Database backup failed. The reason is : *{reason}*

Description

BoD database backup failed for the indicated reason.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8253 – BoD Start Database Backup**Message**

BoD Database backup started.

Description

BoD database backup started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8254 – BoD Finish Database Backup**Message**

BoD Database backup finished.

Description

BoD database backup finished.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8260 – BoD Cluster Reinitialized

Message

The BoD cluster has reinitialized. The indicated blade is now the primary.

Description

The BoD cluster has reinitialized. The specified server is now the primary.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8300 – BoD Send Message | Debug

Message

Sending *{msg type}* to *{cmts ip}* *{msg contents}*

Description

This trace log records all messages sent in BoD. If BoD sessions are created containing CMTSIP, the PCMM requests sent from BoD also contain the CMTSIP. The PCMM requests may be GateSet/GateInfo/GateDelete.

Severity

Info, Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8301 – BoD Receive Message | Debug | Warning**Message**Received *{msg type}* from *{ip address}* *{msg contents}***Description**

The specified message type was received from the specified CMTS (or downstream policy server).

Severity

Info, Debug, Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8302 – BoD Request Timeout**Message***{req}* request to *{ip address}* timed out

Description

The specified request to the specified element has time out.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8310 – BoD PCMM Incorrect Service XML Syntax

Message

Incorrect XML syntax in PCMM services file *{file name}##{error msg}*

Description

Incorrect XML syntax in PCMM services file.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8311 – BoD PCMM Miss Required Fields

Message

Missing required fields for services *{service name}*#Details:#{*details*}

Description

Missing fields required for services.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8312 – BoD Diameter Incorrect Service XML Syntax

Message

Incorrect XML syntax in Diameter services file *{file name}*#{*details*}

Description

Incorrect XML syntax in Diameter services file.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8313 – BoD Duplicate Service

Message

Services or service indexes already exists#Details:#{details}

Description

Services or service indexes already exist.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8314 – BoD Service Multiple Used

Message

Same services or service indexes used multiple times#Details:#{details}

Description

Same services or service indexes used multiple times.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8315 – BoD Active Session Existed**Message**Active session exists for service(s): *{service name}***Description**

Active session exists for the specified service.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8320 – BoD PCMM Create Session Failed**Message**PCMM error encountered for creating session with duration = *{time}*, this is a recoverable error, scheduling a retry for gate set, sessionId = *{sess id}*, retry attempt *{num}*.**Description**

BoD PCMM failed to create a session. A retry is scheduled.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8321 – BoD PCMM Delete Session Failed

Message

PCMM error encountered for deleting session, scheduling a retry for gate deletion, sessionId = {*sess id*}, retry attempt {*num*}.

Description

BoD PCMM encountered an error when deleting the session. A retry is scheduled.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8400 – BoD MAC Translation Failed Due to Session ID Connection Failed

Message

MAC Translation failed due to connection failure for session ID {*sess id*}: MAC address: {*mac address*} {2}.

Description

MAC Translation failed due to connection failure.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8401 – BoD MAC Translation Succeeded**Message**

MAC Translation succeeded for session ID *{sess id}* on retry attempt *{num}*. MAC address: *{mac address}*. Translated IP address: *{ip address}*.

Description

BoD succeeded in translating the MAC address for the session ID.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8402 – BoD MAC Translation Failed Due To No IP Address For Session ID

Message

MAC Translation failed due to no IP Address returned for session ID *{sess id}*: MAC address: *{mac address}* {2}.

Description

MAC Translation failed due to no IP Address returned for session ID.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8403 – BoD MAC Translation Failed Due To Response Failed For Session ID

Message

MAC Translation failed due to response parse failure for session ID *{sess id}*: MAC address: *{mac address}* {2}.

Description

MAC Translation failed due to response parse failure for session ID.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8404 – BoD MAC Translation Failed Due To Incorrect MAC Translation URL for Session ID**Message**

MAC Translation failed due to incorrect MAC Translation URL for session ID *{sess id}*:
MAC Translation URL: *{mac trans ip} {2}*.

Description

MAC Translation failed due to incorrect MAC Translation URL for session ID.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8405 – BoD MAC Translation Failed Due To MAC Address Connection Failure**Message**

MAC Translation failed due to connection failure for MAC address: *{mac address}*.

Description

MAC Translation failed due to connection failure for specified MAC address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8406 – BoD MAC Translation Failed Due To No IP Address For MAC Address

Message

MAC Translation failed due to no IP Address returned for MAC address: *{mac address}*.

Description

MAC Translation failed due to no IP address for specified MAC address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8407 – BoD MAC Translation Failed Due To Response Failed For MAC Address

Message

MAC Translation failed due to response parse failure for MAC address: *{mac address}*.

Description

MAC Translation failed due to parse failure for MAC address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8408 – BoD MAC Translation Failed Due To Incorrect MAC Translation URL For MAC Address

Message

MAC Translation failed due to incorrect MAC Translation URL for MAC Translation URL: {mac address}.

Description

MAC Translation failed due to incorrect MAC Translation URL for MAC Address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8410 – BoD MAC Translation Failed Due to Configuration Error

Message

MAC Translation failed due to configuration error.

Description

A configuration error caused the MAC Translation to fail.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8411 – BoD Session Notification Return Success

Message

Notification for *{sess id}* is sent to *{ip address}*.

Description

BoD session notification returns success.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8412 – BoD Session Notification Return Other Status

Message

Server returns *{status}* when send notification *{sess id}* out.

Description

Server returns *status* when notification sent out.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8413 – BoD Session Notification Expire

Message

Notification for *{sess id}* expired *{time}*.

Description

The notification for the session id expired at the indicated time.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8414 – BoD Session Notification Retry

Message

Notification retry *{sess id}*.

Description

Notification retried.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8420 – IPv6 Subnets Filtering Stats

Message

{server}: Discovered IPv6 subnets were filtered for CMTS(*{ip address}*), Before:*{num}*;
After:*{num}*

Description

On CMP server or DC, the discovered subnets were filtered on a certain CMTS, and show the number of subnets before and after the filtering.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP, DC

Group

N/A

Recovery

1. No action required.

8421 – IPv6 Subnets Filtering Stats All**Message**

{server}: Discovered IPv6 subnets were filtered for all CMTS, Before:*{num}*; After:*{num}*

Description

On CMP server or DC, the discovered subnets were filtered on all the CMTS, and show the number of subnets before and after the filtering.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP, DC

Group

N/A

Recovery

1. No action required.

8422 - IPv6 Subnets Aggregation Stats**Message**

{server}: Discovered IPv6 subnets were aggregated for CMTS(*{cmts ip}*), Before:*{num}*; After:*{num}*

Description

On CMP server or DC, the discovered subnets were aggregated on a certain CMTS and show the number of subnets before and after the aggregation.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP, DC

Group

N/A

Recovery

1. No action required.

8423 - IPv6 Subnets Aggregation Stats All

Message

{server}: Discovered IPv6 subnets were aggregated for all CMTS, Before:*{num}*; After:
{num}

Description

On CMP server or DC, the discovered subnets were aggregated on all the CMTS and show the number of subnets before and after the aggregation.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP, DC

Group

N/A

Recovery

1. No action required.

8424 – IPv6 Subnets Setting To MA Success

Message

IPv6 subnet settings were deployed to *{num}* MA(s), *{num}* successful, *{num}* fail.*{3}*

Description

IPv6 subnet settings were deployed to all MAs successfully.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

MA

Recovery

1. No action required.

8425 – IPv6 Subnet Setting To MA Failure**Message**

IPv6 subnet settings were deployed to *{num}* MA(s), *{num}* successful, *{num}* fail.{3}

Description

IPv6 subnet settings were deployed and some MAs failed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

MA

Recovery

1. Reapply on corresponding MA by the content of trace log.

8426 – Subnets Overlapped | Details**Message**

Total of *{num}* subnets duplicate or overlapping.

Total of *{num}* subnets duplicate or overlapping. Details:#{*details*}

Description

Subnets are duplicated or overlapping in the CMTS.

Severity

Warning

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8427 – Subnet Overlap Detect Task Start

Message

Starting Subnet Overlap Detecting task.

Description

The task to detect duplicate or overlapping subnets in the CMTS has started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery:

1. No action required.

8428 – Subnet Overlap Detect Task End

Message

Finishing Subnet Overlap Detecting task.

Description

The task to detect duplicate or overlapping subnets in the CMTS has ended.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery

1. No action required.

8429 – IPv4 Subnets Filtering Stats All

Message

{0}: Discovered IPv4 subnets were filtered for all CMTS, Before:*{1}*; After *{2}*.

Description

The IPv4 subnets filtering stats.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery:

1. Go to **Global Configuration Settings > Route by CMTS IP**.
2. Set the value of **Route by CMTS IP** to **True**.
3. Go to **System Administration > Scheduled Tasks**.
4. Run Subnet SNMP Collector.

8430 – IPv4 Subnets Filtering Stats

Message

{0}: Discovered IPv4 subnets were filtered for CMTS(*{3}*), Before:*{1}*; After:*{2}* .

Description

The IPv4 subnets filtering stats.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery:

1. Go to **Global Configuration Settings > Route by CMTS IP**.
2. Set the value of **Route by CMTS IP** to **True**.
3. Go to **System Administration > Scheduled Tasks** .
4. Run Subnet SNMP Collector.

8431 – OSSI Triggered CMTS Rediscovery

Message

OSSI triggered CMTS rediscovery: *{0}* successful, *{1}* failed. *{2}*

Description

The OSSI triggered CMTS rediscovery trace log includes the discovery success count and the discovery failure count.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery:

1. For a CMTS discovery failure, send an OSSI request to query the CMTS and trigger rediscovery. Refer to *OSSI XML Interface Definitions Reference* for more information.

8432 – Subnets Overlapped CMTS Details

Message

Compare CMTS {0} ({1}) subnets overlap with above CMTSs, Learned IPv4 Subnets: {2}, Learned IPv6 Subnets:{3}, Total IPv4 Subnets:{4}, Total IPv6 Subnets:{5}, Duplicate/Overlapping IPv4 Subnets {6}, Duplicate/Overlapping IPv6 Subnets {7}.
Details:
{8}

Description

The task to detect duplicate or overlapping subnets in the detailed CMTS.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

N/A

Recovery

1. No action required.

8500 – MA Server Start

Message

MA Server started

Description

MA server has started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Deprecated ID

3

Recovery

1. No action required.

8501 – BoD HTTP Request Fail

Message

HTTP request failed: *{sess id}#{error msg}*

Description

The HTTP request failed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Deprecated ID

21

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8502 – BoD Classifier Active SubIP**Message**

Classifier already active for SUBIP={sub ip}; SUBPORT={sub port}; DESTIP={dest ip}; DESTPORT={dest port} - request ignored.

Description

The classifier is already active for the specified subscriber IP address. The request is ignored.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Deprecated ID

24

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8503 – BoD PS Conn Drop

Message

Policy server connection dropped from *{ip address}*. BoD has scheduled policy server reconnect task.

Description

The Policy server connection was dropped. BoD has scheduled a reconnect task.

Severity

Alert

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8504 – BoD Disconn

Message

Disconnected policy server connection *{ip address}*

Description

BoD disconnected the policy server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

-
1. If the problem persists, contact [My Oracle Support](#).

8505 – BoD Disconn Fail

Message

Disconnection failure from policy server *{ip address}*

Description

The BoD failed to disconnect the policy server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8506 – BoD Conn Fail

Message

Could not establish policy server connection to *{ip address}*

Description

The BoD could not establish a connection.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8507 – BoD DB Auto Delete Start

Message

BoD has reached the maximum number of historic sessions (*{num}*) allowed in the BoD database. BoD is minimally auto-deleting the oldest *{num}* sessions to get back to this limit.

Description

BoD has exceeded the maximum number of sessions and will delete the minimum number of oldest sessions to return to the threshold.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8508 – BoD DB Auto Delete End

Message

BoD has completed the auto-deletion of the oldest historic sessions in the BoD database; *{num}* historic sessions have been deleted. It is recommended you perform a database backup to reduce the size of your database before the next auto-delete occurs.

Description

BoD has completed the auto-deletion of the oldest historic sessions in the BoD database; the specified number of historic sessions have been deleted. It is recommended you perform a database backup to reduce the size of your database before the next auto-delete occurs.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8509 – BoD Send Debug**Message**Sending *{info}* to *{dest ip}* {2}**Description**

BoD sending the specified information to the specified locations.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8510 – BoD Received Info**Message**Received *{info}* from *{location}* {2}

Description

BoD received the specified information from the specified locations.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8511 – BoD Received Warn

Message

Received *{warning}* from *{location}* {2}

Description

BoD received the specified warning from the specified locations.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8512 – BoD MAC Translate Success

Message

MAC Translation succeeded for session ID *{sess id}* on retry attempt *{num}*. MAC address: *{mac address}*. Translated IP address: *{trans ip}*.

Description

The BoD successfully translated the specified MAC address to the indicated IP address for the specified session.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8513 – BoD MAC Translate IP Fail

Message

MAC Translation failed due to no IP Address returned for session ID *{sess id}*: MAC address: *{mac address}* *{2}*.

Description

The BoD failed to translate the specified MAC address for the indicated session.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8514 – BoD MAC Translate Parse Fail

Message

MAC Translation failed due to response parse failure for session ID *{sess id}*: MAC address: *{mac address}* *{error msg}*.

Description

The BoD failed to translate the specified MAC address because of a response parse failure for the specified session.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8515 – BoD MAC Translate MAC Fail

Message

MAC Translation failed due to incorrect MAC Translation URL for session ID *{sess id}*: MAC Translation URL: *{trans ip}* *{error msg}*.

Description

MAC translation failed due to incorrect MAC Translation URL for the specified session.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8516 – BoD MAC Translate Conn MAC Fail**Message**MAC Translation failed due to connection failure for MAC address: *{mac address}*.**Description**

MAC Translation failed due to connection failure for the specified MAC address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8517 – BoD MAC Translate IP MAC Fail**Message**MAC Translation failed due to no IP Address returned for MAC address: *{mac address}*.

Description

MAC Translation failed because no IP Address was returned for the specified MAC address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8518 – BoD MAC Translate Parse MAC Fail

Message

MAC Translation failed due to response parse failure for MAC address: *{mac address}*.

Description

MAC Translation failed because of a response parse failure for the specified MAC address.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8519 – BoD MAC Translate Incorrect MAC Fail

Message

MAC Translation failed due to incorrect MAC Translation URL for MAC Translation URL: *{trans ip}*.

Description

MAC Translation failed due to incorrect MAC Translation URL.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8520 – Bod Service Parse Fail

Message

RDR: Failed to parse service index: *{index}*. Skipping this RDR.

Description

RDR failed to parse the specified service index. This RDR will be skipped.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8521 – BoD Socket Closed

Message

RDR: Client or Server has closed the socket connection

Description

The client of server has closed the socket connection.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8522 – BoD RDR Start Error

Message

RDR: Error starting RDR service on port *{port num}*. Error is: *{error msg}*

Description

BoD encountered an error while starting the RDR service on the indicated port.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8523 – BoD RDR Port Busy**Message**RDR: port *{port num}* busy, retrying. Attempt number: *{num}***Description**

The RDR service port is busy. BoD will retry. The number of the attempt is indicated.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8524 – BoD RDR Fatal Error**Message**RDR: Fatal error starting RDR service on port *{port num}***Description**

Bod encountered a fatal error while starting the RDR service on the indicated port.

Severity

Critical

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8525 – BoD Start MSG Processing Debug

Message

RDR: Start message processing {0}

Description

Start message processing

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8526 – BoD Stop MSG Processing

Message

RDR: Stop message processing {0}

Description

Stop message processing

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8527 – BoD Start MSG Processing Info**Message**

RDR: Start message processing {0}

Description

Info level log generated when RDR service starts message processing.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8528 – Edge OAM Device Discovered**Message**

Edge QAM Device {0} discovered from the policy server {ip address}

Description

The BoD discovered the specified Edge OAM device.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8529 – PCMM Send AM Info

Message

PCMM: Sending *{msg type}* to AM *{ip address:port}* Details: *{details}*

Description

The specified message type was sent to the specified AM (or upstream policy server).

Note: This message is logged at the Warning level when the PCMM message type is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

Severity

Info

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Deprecated ID

1013

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8530 – PCMM Receive

Message

PCMM: Received *{msg type}* from *{DownstreamPS ip address:port}* *{2}*

Description

The specified message type was received from the specified CMTS (or downstream policy server).

Note: This message is logged at the Warning level when the PCMM message is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

Severity

Info

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

PCMM

Deprecated ID

1012

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8531 – DQOS Send CMS Info

Message

DQOS: Sending *{msg type}* to CMS *{ip address}*

Description

The specified message type was sent to the specified CMS.

Note: This message is logged at the Warning level when the DQOS message is an error message such as GateSetErr, GateDeleteErr, or GateInfoErr, and logged at the Info level when the message is an ACK such as GateSetAck, GateInfoAck, or GateDeleteAck.

Severity

Info

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

DQOS

Deprecated ID

1113

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8532 – SPC DQOS Send CMS Info

MessageSPC DQOS: Sending *{msg type}* to CMS *{ip address}***Description**

The specified message type was sent to the specified CMTS. If the message is reporting an error, then this message is logged at the Warning level, otherwise it is logged at the Info level.

Severity

Info

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SPC DQOS

Deprecated ID

1213

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8534 – BoD RDR Quota MSG Processing Debug**Message**RDR: Quota message processing *{msg type}***Description**

BoD is processing a Quota message of the specified type.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8535 – BoD RDR Quota MSG Processing Info**Message**RDR: Quota message processing *{msg type}***Description**

BoD is processing a Quota message of the specified type.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8540 – BoD Received Debug

Message

Received {0} from {1} {2}

Description

BoD received a message of the specified type from the indicated device.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8541 – BoD Start Msg Processing Warn

Message

RDR: Start message processing {0}.

Description

RDR: Started message processing.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8600 – BoD Invalid Session ID Arg**Message**Can't find session from COMCOL which SSID is *{sess id}*.**Description**

BoD cannot find the COMCOL session because the session ID is invalid.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8601 – BoD PCMM Request Reject**Message**Reject PCMM request by load shedding, request type is *{req type}*, reason is *{reason}*.

Description

BoD rejected the PCMM request by load shedding. The request type and reason are indicated.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8602 – BoD PCMM Mode Not Enabled

Message

PCMM mode was not enabled! Can't handle PCMM request *{req type}* for session *{sess id}*!

Description

BoD cannot handle the specified PCMM request type for the indicated session because PCMM mode is not enabled.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8603 – BoD Diameter Mode Not Enabled

Message

Diameter mode was not enabled! Can't handle diameter request *{req type}* for session *{sess id}*!

Description

BoD cannot handle the specified Diameter request type for the indicated session because Diameter mode is not enabled.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

8700 – BoD Admission Protocol Busy Event

Message

ADMISSION: *{svr name}*: Busy : criteria *{threshold}*

Description

The current load on the specified server exceeds the indicated admission criteria thresholds.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. Typically, this condition returns to a normal state. If the problem persists, contact [My Oracle Support](#).

8701 – BoD Admission Protocol Clear Event

Message

ADMISSION: *{svr name}*: Normal : criteria *{threshold}*

Description

The current load on the specified server is below the indicated admission criteria thresholds.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8702 – BoD Admission Component Busy Event

Message

ADMISSION: *{3}*: Resource *{res name}* : new condition *{1}* of the criteria *{threshold}*

Description

The load of the monitored resource is evaluated by an admission controller as exceeding admission criteria threshold.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. Typically, this condition returns to a normal state. If the problem persists, contact [My Oracle Support](#).

8703 – BoD Admission Component Clear Event**Message**

ADMISSION: {3}: Resource {res name} : new condition {1} of the criteria {threshold}

Description

The load of the monitored resource is below clearing criteria threshold.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. No action required.

8704 – BoD PCMM Too Busy Set | Clear**Message**

ADMISSION: {res name} is in a {Busy | Normal} state

Description

The specified resource name is in the indicated state (that is, busy or normal). A busy (or Set event) state triggers a Warning log event; a normal (or Clear event) state triggers an Error log event.

Severity

Warning

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

BoD

Group

BoD

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10000 – ADS Connection Established

Message

ADS: Analytics Data Stream connection to *{ads client}* has been established for Channel: *{chan type}* and Version: *{ads ver}*

Description

A connection established to the MPE device from the specified Analytics client. The channel type and ADS interface version are indicated.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

ADS

Recovery

1. No action required.

10001 - ADS Connection Closed**Message**

ADS: Analytics Data Stream connection to *analytics client id* was closed.

Description

The connection between the MPE device and the Analytics client was closed.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

ADS

Recovery

1. No action required.

10002 - ADS Connection Lost Set | Lost Clear**Message**

ADS: Lost Analytics Data Stream connection to *{analytics client id}*

Description

The connection between the MPE device and the Analytics client was closed due to an error.

Severity

Warning

Notification

Trace Log

Alarm

Yes - 78000

Trap

No

Server

MPE

Group

ADS

Recovery

1. No action required.

10003 – ADS Receive Error

Message

ADS: Error processing Analytics Data Stream message received from *analytics client id. {1}*

Description

The Analytics Data Stream request from the Analytics Client resulted in an error.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

ADS

Recovery

1. No action required.

10004 – ADS Send Error

Message

ADS: Error sending Analytics Data Stream message to *analytics client id. {1}*

Description

An error occurred while sending the Analytics Data Stream message from the MPE device.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

ADS

Recovery

1. No action required.

10005 – ADS Error**Message**

ADS: Analytics Data Stream encountered an error. {0}

Description

An error occurred during the Analytics Data Stream processing.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

ADS

Recovery

1. No action required.

10006 – Sy Receive Notification**Message**SY: Received notification from *sy identity* message:
*diameter_message***Description**

This trace log event indicates that an SNR was received from the OCS and provides the message details.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. No action required.

10007 – Sy Bad Realm

Message

SY: Peer Realm {0}

Description

There is an undefined realm in the Sy configuration.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. Check the configured Realm for the connection.

10008 – Sy Bad Address

Message

SY:{0} address {1}

Description

The primary address in the Sy configuration is undefined.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. Check the configured Address for the connection.

10009 – Sy Search

Message

SY: Searching *sy identity* for subscriber: *subscriber id*

Description

This trace log event indicates that a new SLR search has been started for the given subscriber.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. No actions required.

10010 – SY Search Results

Message

SY: Search results from peer *sy_identity* for subscriber *subscriber_id* are:
policy_counter_values

Description

This trace log indicates a successful SLR/SLA lookup and details the contents.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. No actions required.

10012 – Sy Search Error

Message

SY: Search failure on *sy_identity: {1}*

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. No actions required.

10013 – Bad XML from SPR**Message**

XML Parse Failure from SDM. Subscriber="{0}". {1}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SY

Recovery

1. No actions required.

10014 – TDF Connection Closed**Message**

Unable to set policy for TDF session establishment, destination host={host name}, realm={realm} for TDF {2}

Description

Unable to set policy to establish a traffic detection function (TDF) session for the specified destination. The connection was closed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10015 – Exceeds Max Allowed AVP Conditional Policy Info AVP

Message

More than four Conditional-Policy-Information AVPs provisioned, considering four Conditional-Policy-Information AVPs with earliest Execution-Time.

Description

This tracelog is displayed when there is an attempt to provision more than four instances of Conditional-Policy-Information AVP per CCA/RAR.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Recovery

1. Recheck the policies deployed which provision Conditional-Policy-information AVP in CCA/RAR to make sure no more than four instances are provisioned.
2. If the problem persists, contact [My Oracle Support](#).

10020 – CMP Started

Message

CMP started

Description

The CMP server is started.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No actions required.

10021 – Import XML Add**Message**

Import XML Add {0} executed by {4}

Successful: {1} Failed: {2} Total execution time {3} millisecond

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No actions required.

10022 – Import XML Update**Message**

Import XML Update {0} executed by {4} Successful: {1} Failed: {2} Total execution time {3} millisecond

Description

An XML file was imported that updated data.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No actions required.

10023 – Import XML Delete

Message

Import XML Delete {0} executed by {4} Successful: {1} Failed: {2} Total execution time {3} millisecond

Description

XML file was imported that deleted data.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No actions required.

10024 – Import XML Fail

Message

Import XML Remove {0} From Group executed by {4} Successful: {1} Failed: {2} Total execution time {3} millisecond

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No actions required.

10025 – XML Add Fail

Message

Import XML Add {0} To Group executed by {4} Successful: {1} Failed: {2} Total execution time {3} millisecond

Description

An Add action using XML failed.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP

Group

OSSI

Recovery

1. No actions required.

10026 – RC proxy apply2

Message

Apply *data_type* to MPE (HostName: *ip/hostname*) executed by *user name*
Total execution time *execution time* millisecond

Description

Data type that pushed to an MPE by admin.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Configuration

Recovery

1. No actions required.

10027 – RC proxy apply

Message

Apply *number data_type(s)* to MPE (HostName:*ip/hostname*) executed by *user_name*
Total execution time *execution_time* millisecond.

Description

The number of network elements that pushed data to an MPE by admin.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Configuration

Recovery

1. No actions are required.

10028 – RC proxy send**Message**

Send Message(*message*) to MPE (HostName:*ip/hostname*) executed by *user_name*
Total execution time *execution_time* millisecond

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

CMP/MPE

Group

Configuration

Recovery

1. No actions required.

10029 – Stat Rsync Clean Task Start**Message**

Starting Statistics Rsync Cleanup task.

Description

The Statistics Rsync Cleanup task is starting.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10031 – Diam Service Invalid XML File

Message

Incorrect XML syntax in Diameter services file *file_name*
error_message

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10032 – Stats Sync Task Start

Message

Starting *task name* Task.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No actions required.

10033 – Stats Sync Task Repository Success

Message

name Task was successful for sync local repository to remote server(*ip address*) after retry *{count}* times

Description

The Stats Sync task successfully synchronized the local repository to the specified remote server. The number of attempts is indicated.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10036 – Retry fail

Message

Diameter: PCC/ADC rule {0} retry failed after {1} attempts for subscriber {2} {3}

Description

This trace log is generated when there is an RAA error or if an RAA timeout triggers the last retry RAR attempt.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Check network connectivity. If the problem persists, contact [My Oracle Support](#).

10037 – DBPLUGIN No Match Debug

Message

DBPLUGIN: No matches for *criteria*, search type *id*

Description

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Data Source

Recovery

1. No actions are required

10038 – Email Not Enabled Info

Message

SMTP: SMTP functionality is not enabled to send message. *{svr ip address}*

Description

SMTP functionality is not enabled on the specified server to send notification.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

SMTP

Recovery

1. No actions required.

10039 – RADIUS Server Init

Message

RADIUS: Initializing communications on port *{port}*

Description

RADIUS is initializing communications on the specified port.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. No action required.

10040 – RADIUS Server Start Notice

Message

RADIUS: Started listening on port *{port}*

Description

The RADIUS server has started listening on the specified port.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. No action required.

10041 – RADIUS Drop Invalid Warn

Message

RADIUS: Dropping invalid message *{msg type}*. *{msg details}*

Description

RADIUS is dropping an invalid message.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server
MPE

Group
RADIUS

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10042 – RADIUS Drop Bad MD5 Warn

Message

RADIUS: Dropping message with bad MD5, probably bad password in *{msg type}*

Description

RADIUS is dropping a message with a bad MD5 checksum file.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10043 – RADIUS Sent

Message

RADIUS: Sent *{msg type}* [{*identifier*} / {*sess id*}] to {*ip address:port num*} {*details*}

Description

RADIUS sent a message with the indicated specifications.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. No action required.

10044 – Policy Info Event

Message

Policy Event: *{event message}*

Description

A policy event was logged.

Severity

Info

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

SMTP

Recovery

1. No actions required.

10045 – RADIUS Server Start Fail

Message

RADIUS: Start failed on port *{port}*

Description

RADIUS failed to start on the indicated port.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10046 – RADIUS Received**Message**

RADIUS: Received *message code / accounting type* [pocket id / session id] from client address message

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

RADIUS

Recovery

1. No actions are required

10048 – SCTP Path Status**Message**

Diameter: SCTP path on association ID {0} address {1} {2}

Description**Severity**

Info, Error, Notice

Notification

Trace Log

Alarm

Yes

Trap

No

Server

MPE, MRA

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10100 – Avg Sess Size Exceeds Projected Set

Message

Average session size exceeds the projected session size *size*, current average session size: *size*

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10101 – Avg Sess Size Exceeds Projected Clear

Message

Average session size is below the projected session size *size*, current average session size: *size*

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10102 – Sess Size Reached Threshold Set**Message**

Session database size reached threshold percent of session database capacity *percent*,
current database session size percentage: *percent*

Description**Severity**

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10103 – Sess Size Reached Threshold Clear

Message

Session database size below threshold percent of session database capacity *percent*, current database session size percentage: *percent*

Description

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MPE

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10104 – Avg Bind Size Exceeds Projected Set

Message

Average binding size exceeds the projected binding size *{0}*, current average binding size: *{1}*

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

Admission Control

Recover

1. If the problem persists, contact [My Oracle Support](#).

10105 – Avg Bind Size Exceeds Projected Clear

Message

Average binding size is below the projected binding size *size*, current average binding size: *size*

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10106 – Bind Size Reached Threshold Set

Message

Binding database size reached threshold percent of binding database capacity *threshold*, current binding database size percentage: *size*

Description**Severity**

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MRA

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10107 – Bind Size Reached Threshold Clear

Message

Binding database size is below threshold percent of binding database capacity *size*, current binding database size percentage: *size*

Description

Severity

Warning

Notification

Trace Log

Alarm

Yes

Trap

Yes

Server

MRA

Group

Admission Control

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10108 – ReplicationStats Task Start

Message

Starting Replication Statistics task.

Description

The Replication Statistics task is starting.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10109 – ReplicationStats Task Failed**Message**

Replication Statistics Task failed.

*{0}***Description****Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10110 – ReplicationStats Task Success**Message**

Replication Statistics Task completed successfully.

Description

The Replication Statistics Task completed successfully.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10111 – ReplicationStats Task Finish

Message

Finishing Replication Statistics task.

Description

The Replication Statistics task is finishing.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10112 – ReplicationStats Task Data Available

Message

Replication Statistics collection complete and data is available for request.

Description

Replication Statistics collection is complete. The data is available for request.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10113 – Sy On Demand Policy Action Failure**Message**

SY: Policy Action failure attempting to send *{msg type}* SLR to *{1}* on MPE *{ip address}* for subscriber: *{3}*: *{4}*

Description

SY encountered a policy action failure while attempting to sent a message to the indicated destination.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10114 – Diam Session Cleanup Results

Message

Diameter Session cleanup task is finished and iterated {0} sessions, detected {1} stale sessions, and audited {2} sessions

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10115 – Diameter Invalid Ancids Warning

Message

Diameter:{0} "{1}" for subscriber {2} in {3} is invalid, can not find related AF flow. {4}

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10116 – PCEF Report Timeout

Message

PCRF waiting PCEF reporting timeout for AF: {0} : {1}
{2}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

DC

Group

Data Collection Task

Recovery

1. No action required.

10117 – Subtrace Disabled Busy State

Message

Subscriber Activity Logging has been temporarily disabled due to transition to Busy state.

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Recovery

1. No action required.

10118 – Subtrace Enabled Normal State

Message

Subscriber Activity Logging has been enabled due to transition to stable state.

Description

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Recovery

1. No action required.

10119 – X1 Connection Lost

Message

X1 Connectivity from Mediation Function: {0} with MPE: {1} lost.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Lawful Intercept

Recovery

1. Diagnose the X1 Connection between the MF and Policy Server.
2. If problem persists contact [My Oracle Support](#).

10120 – Duplicate Default Bearer Rule**Message**

Duplicate default bearer rules detected with precedence {0}:
{1}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

10121 – Invalid Traffic Profile**Message**

Invalid traffic profile: {profile id}

Description

The specified traffic profile is invalid.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

10122 – X2 Connection Lost

Message

X2 Connectivity from MPE {0} with Mediation Function {1} lost.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Diagnose the X2 Connection between the MF and Policy Server.
2. If problem persists contact [My Oracle Support](#).

10123 – Policy Logging Overflow

Message

Policy logging has overflowed, data will be missing after this time.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10124 – Subtrace Policy Logging Overflow**Message**

Subscriber Tracing has overflowed, data will be missing after this time.

Description

The logging of subscriber tracing data has overflowed. Data will be missing after this event's time.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10125 – AN GW Failed**Message**

An-Gw failure for: {0}

Description

The AN-GW encountered an error.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10126 – Max Wait Time Exceeded

Message

Request Maximum Wait Time has Exceeded, This Request is ignored.
{0}

Description

The request exceeded the maximum wait time. The request is ignored.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Verify NTP consistency across the network.
2. Check for misbehaving network element.
3. If the problem persists, contact [My Oracle Support](#).

10127 – Diameter Newer Session Detected

Message

A newer session is detected, This Request is rejected with
DIAMETER_NEWER_SESSION_DETECTED.
{0}

Description

A more recent session has been detected. This request is rejected.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. Verify NTP consistency across the network.
2. Check for misbehaving network element.
3. Verify that a race condition does not exist between multiple PGWs.
4. If the problem persists, contact [My Oracle Support](#).

10128 – SY Reconciliation Status

Message

SY: Reconciliation Status: {0}

Description

This trace log indicates the current status of the Sy Reconciliation task.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10129 – Sy Reconciliation Stats

Message

SY: Reconciliation Stats: Total Session Audited: *{0}*

Description

This trace log indicates the statistics about the most recent pass of the Sy Reconciliation task, only if the status is Stopped or Complete.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10130 – Unauthorized Non Emergency Session

Message

Reject a non-emergency request *{0}* from AF binding to an emergency APN: *{1}*

Description

This trace log is triggered when a non-emergency Rx session binding to an emergency APN is requested.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10131 – PCEF Initiated Emergency Request**Message**Reject a PCEF-initiated emergency request *{0}* to an emergency APN: *{1}***Description****Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10132 – Sy Reconciliation QP Notif**Message**SY: Notify of split-brain resolved. Split-brain start time: *{0}***Description**

Notification of split brain recovery was received by the MPE device from the QP with the time stamp for when the QP believes the event began.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10133 – SYNC MRA Session Binding

Message

Cleanup *{0} session id or PDN connection* in message *{1} message type* with result code *{2} message result code*.

Description

Trigger if a session binding or PDN connection is cleaned up when receiving Gx RAA with rc=5002 or Rx AAA with rc=5065.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact server.

10135 - High Bandwidth Attempt

Message:

The attempt of bandwidth greater than $2^{32}-1$ bps when PCEF not support Extended-BW-NR feature. \nSession Id: {0} \nBandwidth attempted: {1} \nValue: {2}

Description:

Displays when there is an attempt to add bandwidth greater than $2^{32}-1$ bps but the PCEF is not support Extended-BW-NR feature.

Severity:

Warning

Notification:

Warning

Alarm:

Normal

Trap:

None

Server:

MPE

Group:

Diameter

Recovery:

1. If the problem persists, contact My Oracle Support.

10140 – Diameter App Not Found Message

Message

Diameter: Application {0} not found among running applications.

Description

The specified application was not found among the running applications.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10141 – Diameter Peer Config Fail

Message

Diameter: Peer Configuration Failure. {0}

Description

The specified Diameter Peer configuration failed.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10160 – Diam Invalid App Detect Info Warning

Message

Diameter:{0} AVP in {1} is missing in Application-Detection-Information AVP. {2}

Description

The specified Diameter AVP in the specified device is missing in the Application-Detection-Information AVP.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. If the problem persists, contact [My Oracle Support](#).

10200 – VNF server create**Message**VNF: Creating Instance: *{VNFC details}***Description**

The VNFC details include the Cluster Name (VNF), Server Name (Instance), Network Addresses, Config Drive enabled, Flavor, Host ID, Instance ID, Image, Security Groups, Status, Tenant ID, User ID, and Availability Zone being created.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:**10201 – VNF server update****Message**

VNF: Updating Instance:
Previous Instance: *{VNFC_details}*
Updated Instance *{VNFC_details}*

Description

The VNFC details include the Cluster Name (VNF), Server Name (Instance), Network Addresses, Config Drive enabled, Flavor, Host ID, Instance ID, Image, Security Groups, Status, Tenant ID, User ID, and Availability Zone begin updated.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:

10202 – VNF server delete

Message

VNF: Removing Instance: *{VNF name}*

Description

The name of the VNFC being removed.

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:

10203 – VNFMGR get

Message

VNF: Retrieving data for id: *{VNF name}*

Description

Returns VNFC details for VNF instances.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:**10204 – VNF MGR get error****Message**VNF: Retrieving data for id: *{VNF name}***Description**

Name of the VNF where a data retrieve failure occurred.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:**10205 – VNF operation error set****Message**VNF: Operation: *{POST/PUT/DELETE}* Error Instance: *{VNF name}* HTTP Operation: *{GET/POST/PUT/DELETE}* HTTP Error: *{Error from HTTP Operation}* HTTP URI: *{URI of HTTP request}* HTTP Answer: *{Response data}* VIM Error: *{Error msg from VIM}*
Instance Data: *{VNF details}***Description**

A VNF operation caused a failure.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:

10206 – VNF operation error clear

Message

VNF: Operation Alarm Cleared: *{VNF name}* Instance Data: *{VNF details}*

Description

Alarm 78850 - Create, update, or delete operation failed on the VNF cluster - has been cleared.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:

10207 – VNF rest operation

Message

VNF: REST Operation: *{GET/POST/PUT/DELETE}* URI: *{URI of operation}* Data: *{Msg data}*

Description

An outbound REST operation has been attempted.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:**10208 – VNF API unsupported version****Message**

VNF: API Version unsupported: *{API name}* Configured Port: *{API port}* Handler Configured Version: *{API version from configuration}* API Version Data: *{Retrieved API version data}*

Description

The configured version of a REST API being used is not supported by the end server.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:**10209 – VNF Operation Error**

Message

VNF: Error: Operation: {0}

Details:

{1}

Description

Error in the VNF operation.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

VNF

Group

Diameter

Recovery:

10210 – POI Incoming Request

Message

VNF-POI: Incoming: Resource: {0}, Operation:{1}, TaskID; {2}

Data:

{3}

Description

The accepted incoming request from POA.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

VNFMGR

Group

NA

Recovery: No action is required.

10211 – POI Outgoing Request to PPI

Message

VNF-POI: TaskId: {0},
PPI Operation; {1}, PPI Component Data;
{2}

Description

The PPI request send by POI to PPI.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

VNFMGR

Group

NA

Recovery: No action is required.

10212 – POI Return Response to POA

Message

VNF-POI: Returning: Resource: {0}, Operation; {1}, TaskId; {2}
Data:
{3}

Description

The return message to POA.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

VNFMGR

Group

NA

Recovery: No action is required.

10213 – POI Operation Error

Message

VNF-POI: Error occurs in task: *task_name* Error description: *description*

Description

An error occurred in the named task. The error description is displayed. (The description can be a stack trace.)

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

VNFMGR

Group

NA

Recovery:

1. Contact [My Oracle Support](#).

10214 – Rest Response

>

Message

VNF:REST received Response: *response_namr* URI: *uri* Response: *response*

Description

The VNF received a REST response of type *response_namr*. The request and response are displayed.

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

VNFMGR

Group

NA

Recovery: No action is required.**10215 – POI Operation Error**

>

MessageVNF:PPI Error: Operation: *operation_name* Details: *details***Description**

An error was returned for the named operation. The error is displayed.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

VNFMGR

Group

NA

Recovery: No action is required.**11001 – Remote Diversion Set | Clear****Message**

Remote diversion is not possible, alarm {0}

Description

This trace log occurs when all other associated MRA devices are currently unavailable for remote diversion. The Clear event occurs when MRA devices become available.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group

Diameter

Recovery

1. No action is required.

15000 – SCMP Sync Trace Succ

Message

S-CMP reference sync succeeded.

Description

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15010 – SCMP Init Succ

Message

S-CMP {0} initialization succeeded.

Description

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15101 – Mediation SPR Connection Exception**Message**

SOAP: SPR {0} connection exception: {1}

Description**Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15102 – Mediation SPR Connection Timeout**Message**

SOAP: SPR {0} connection time out.

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Mediation

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15103 – Mediation SOAP Parameter Error

Message

SOAP: Mediation SOAP interface parameter error: {0}.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

MF

Recovery

1. No action required.

15104 – Mediation Open COMCOL Error

Message

SOAP: {0}: Could not open database,the usrId is: {1}.

Description**Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15105 – Mediation Operate COMCOL Error

Message

SOAP: {0}: fail to oprate db,the usrId is: {1}, the oprateType is: {2}.

Description**Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15106 – Mediation SOAP Result Error

Message

MEDIATION: Mediation SOAP request get error result, resultcode: {0},UsrId: {1},oprateType: {2}.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15107 – Mediation SPR Connection Request

Message

MDF: Sent SPR message {0} to SPR {1}.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15108 – Mediation SPR Connection Response**Message**

MDF: Received SPR message {0} received from SPR {1}.

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15109 – Mediation SOAP Request**Message**

SOAP: Receiving SOAP operation {0}.

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15110 – SPR Connection Failed

Message

SPR: Create connection to SPR {0} failed.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15111 – SPR Connection Failed Clear

Message

SPR: Create connection to SPR {0} successfully.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15112 – SPR License Limit Set**Message**

MEDIATION: Achieve 80% maximum number of users in SPR.

Description

The mediation server has reached 80% of the maximum number of users in SPR.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15113 – SPR License Limit Clear**Message**

MEDIATION: Below 80% maximum number of users in SPR.

Description

The mediation server is now below 80% of the maximum number of users in SPR.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15114 – SPR Timeout Error

Message

MEDIATION: HandleReply failed for timeout,UserId is: {0},operateType is: {1}.

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15115 – Mediation Admission Protocol Busy Event

Message

ADMISSION: {0}: Busy : criteria {1}

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15116 – Mediation Admission Protocol Clear Event**Message**

ADMISSION: {0}: Normal : criteria {1}

Description**Severity**

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15117 – Mediation Admission Component Busy Event**Message**

ADMISSION: {3}: Resource {0} : new condition {1} of the criteria {2}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15118 – Mediation Admission Component Clear Event

Message

ADMISSION: {3}: Resource {0} : new condition {1} of the criteria {2}

Description

Severity

Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15119 – Mediation SOAP Too Busy Set | Clear

Message

ADMISSION: {0} is in a {1} state

Description

The SOAP interface state of the Mediation server has either changed from normal (not busy) to busy or from busy to normal (not busy).

Severity

Warning/Notice

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15120 – Mediation SOAP Response**Message**SOAP: SOAP response message: *{0}*.**Description****Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15121 – Sync Server Error**Message**Sync: Exception has occurred in sync server: *server*

Description

An exception has occurred in the sync server.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15122 – Sync Stop Server Error

Message

Sync: Could not stop *server* component: *component*

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15123 – Sync Thread Uncaught Exception

Message

Sync: Sync Thread-*server*, uncaught exception: *exception*

Description**Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15124 – Sync Exec CMD Fail

Message

Sync: Command *command* executes failure

Description

The command failed to execute.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15125 – Sync Exec CMD Error

Message

Sync: Exception occurred while executes command *type: command*

Description

An exception occurred while the specified command was executed.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15126 - Sync Accept App Sync Request

Message

Sync: Accepted apply sync request: *request*.

Description

The apply sync request is accepted.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15127 - Sync Reject App Sync Request**Message**Sync: Sync busy at *request*, reject apply sync request.**Description**

The sync server is busy. The apply sync request is rejected.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15128 - Sync App Sync Request Exception**Message**Sync: Exception occurred while process apply sync request: *request***Description**

An exception occurred while processing the apply sync request.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15129 - Sync App Sync Response

Message

Sync: Received apply sync response: *type. response*

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15130 - Sync App Sync Response Exception

Message

Sync: Exception occurred while process apply sync response: *type*

Description

An exception occurred while processing the apply sync response.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15131 - Sync TooBusy Reject Request**Message**Sync: Sync server too busy, reject sync request: *type***Description**

The sync server is too busy. The sync request is rejected.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15132 - Sync Invalid Request**Message**Sync: Invalid sync request: *type***Description**

The sync request is invalid.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15133 – Sync Handle Request Exception

Message

Sync: Exception occurred while process sync request: *type*

Description

An exception occurred while processing the sync request.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15134 - Sync Accept Sync Request

Message

Sync: Accepted sync request: *type*.

Description

The sync request is accepted.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15135 - Sync Open COMCOL Fail**Message**Sync: Failed to open database *type: database***Description**

The sync operation failed to open the database.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15136 - Sync Close COMCOL Fail**Message**Sync: Failed to close database *type: database***Description**

The sync operation failed to close the database.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15137 – Sync Verify Success

Message

Sync: Verify {0} success

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15138 - Sync Verify Fail

Message

Sync: Failed to verify *type: database*

Description

The sync operation failed to verify the database type.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15139 – Sync Resolve Success**Message**

Sync: Resolve conflict success

Description

The sync operation has successfully resolved a conflict.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15140 - Sync Resolve Fail

Message

Sync: Failed to resolve conflict: *type*

Description

The sync operation failed to resolve a conflict.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15141 – Sync Create DATS Success

Message

Sync: Create sync {0} -data files success

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

15142 - Sync Create DATS Fail**Message**

Sync: Failed to create {0}-data files: {1}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15143 - Do Sync Fail**Message**

Sync: Failed to do sync, {type}:{file}

Description

The sync failed. All errors that occur during the synchronization procedure will be reported in the trace log. Examples:

1. failover: already waited *time* ms, but server is still not ready.
2. receiving: reports can't fully received during *time* seconds.
3. timeout: task can't be completed during *time* s.
4. failover: failed to do sync after failover, can't write data to *request file*.
5. failover: can't upload data: *reason*.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15144 - Sync Create Sync Response

Message

Sync: Created sync response: {0}

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15145 – Sync Handle Response Exception

Message

Sync: Exception occurred while process sync response: {0}

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15146 - Sync Disk Quota Exceed**Message**

Sync: Backup folder disk quota exceeds. Disk quota: {0}, total usage: {1}.

Description**Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15147 – Sync Disk No Space**Message**

Sync: No space left on device: {0} "REMAINING"

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15148 – Sync Disk No Space Clear

Message

Sync: Disk space cleaned on device: {0}, cleaned {1} files, released {2} disk spaces.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15149 – MRA Sig Device Filter Changed

Message

MRA Sig device filter changed from *{prev value}* to *{new value}*

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MRA

Group**Recovery**

1. No action required.

15150 –Reject Non-Authorized Connection**Message**

DRA: Rejecting non-authorized *{0}*, no associate *{1}* found.

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server**Group****Recovery**

1. No action required.

15151 – Accept Authorized Connection

Message

DRA: Accepted authorized {0}.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Group

Recovery

1. No action required.

15152 – Retransmit Message

Message

Diameter: Rerouted {0} to {1} ({2} attempts)

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Group

Recovery

1. No action required.

15153 – MPE Sig Device Filter Changed

Message

MPE Sig device filter changed from {prev value} to {new value}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group**Recovery**

1. No action required.

15160 – Batch Operation Error**Message**

Batch: Exception has occurred in batch operation:{0}.

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15161 – Batch Request Validation

Message

Batch: validation result of batch request, data file name: *{0}*, operation time: *{1}*, result: *{2}*.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15162 – Batch Handle Result

Message

Batch: Finished handling task: *{0}*, totally processed: *{1}* lines, successfully processed *{2}* lines, time consumed: *{3}*, ACK file: *{4}*.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15163 – Batch Disk Quota Exceed

Message

Batch: Batch folder disk quota exceeds. Disk quota: {0}, total usage: {1}.

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15164 – Batch Disk No Space

Message

Batch: No space left on device: {0}. "REMAINING"

Description**Severity**

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15165 – Batch Clean Up

Message

Batch: Clean up batch "DIRECTORY" {0}, cleaned {1} files, released {2} disk spaces.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15166 – Scheduled Task RAR Sent

Message

Scheduled: RAR sent for user {0}, for task {1}

Description

Severity

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15167 – Rebuild Diameter Peers**Message**Diameter: Rebuild node(*{0}*) peers*{1}*

=>

*{2}***Description****Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Provision

Recovery

1. No action required.

15200 – PM Gen Stats Sync Task Start**Message**Starting *{0}* Task.**Description****Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15201 – PM Gen Stats Sync Task Success

Message

{0} Task completed successfully.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15202 – PM Gen Stats Sync Task Fail

Message

{0} Task failed.

{1}

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15203 – PM Gen Stats Sync Task End**Message**

Finishing {0} Task.

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15204 – PM Stats Sync Task Start**Message**

Starting {0} Task.

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15205 – PM Stats Sync Task Success

Message

{0} Task completed successfully.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15206 – PM Stats Sync Task Fail

Message

{0} Task failed.

{1}

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15207 – PM Stats Sync Task End**Message**

Finishing {0} Task.

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15208 – PM Stats Sync Task Repository Success**Message**

{2} Task was successful for sync local repository to remote server({1}) after retry {0} times

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15209 – PM Stats Sync Task Repository Fail

Message

{2} Task still failed for sync local repository to remote server(*{1}*) after retry *{0}* times

Description

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. If the problem persists, contact [My Oracle Support](#).

15301 – SMS Stats Sync Task Start

Message

Starting {0} Task.

Description

Starting SMS Notification Statistics Uploading Task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery:

1. No action.

15302 – SMS Stats Sync Task Success**Message**

{0}Task completed successfully.

Description

SMS Notification Statistics Uploading Task completed successfully.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery:

1. No action.

15303 – SMS Stats Sync Task Fail

Message

{0} Task failed.

{1}

Description

SMS Notification Statistics Uploading Task Failure(s):

1. Error in network I/O
2. Error in file I/O
3. Timeout in data send/receive
4. Invalid user name and password.
5. Unknown error. Actual FTP exit code is {}

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery:

1. No action.

15304 – SMS Status Sync Task End

Message

Finishing {0} Task.

Description

Finishing SMS Notification Statistics Uploading Task.

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery:

1. No action.

15305 – SMS Stats Sync Task Repository Success**Message**

*{2}*Task was successful for sync local repository to remote server *{1}* after retry *{0}* times.

Description

SMS Notification Statistics Uploading Task was successful by sync local repository to remote server after 2 retries.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery:

1. No action.

15306 – SMS Stats Sync Task Repository Fail**Message**

{2} Task still failed for sync local repository to remote server *{1}* after retry *{0}* times.

Description

SMS Notification Statistics Uploading Task failed for sync local repository to remote server after 3 retries.

Severity

Error

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery:

1. No action.

17000 – Quota usage daily reset complete

Description: Completed KT usage daily reset.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

1. No action required.

17001 – Quota usage daily reset task start

Description: Starting usage daily reset task.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

1. No action required.

17002 – Quota usage daily reset task is ready to send RARs.

Description: Finished iterating the database. Starting to send RARs to suspect session.

Severity: Info

Notification: Trace Log

Alarm: No

Trap: No

Server: MPE

Group: Diameter

Recovery:

1. No action required.

17100 – MDF Soap Result Error

Message

MDF: SOAP request {0} error result: {1}.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17102 – MDF Soap Parameter Error

Message

MDF: SOAP request parameter error: {0}.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17103 – MDF No QP Name Error

Message

MDF: Add.{0}({1}): cannot get quota profile name.

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17104 – MDF Soap Illegal OPMD Change

Message

MDF: SOAP request illegal opmd change: {0} -> {1}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17105 – MDF Soap Client Result Error**Message**MDF: SOAP client request(*{0}*) error result: *{1}*.**Description****Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17106 – MDF Cannot Parse SDM Response

Message

MDF: SDM client cannot parse SDM response {0}: {1}

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17107 – MDF IMSI Not In Range

Message

MDF: Cannot {0} - not in SPR IMSI range

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17108 – MDF Soap Client Request

Message

MDF: Sent request to MGW: {0}

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17109 - MDF Soap Client Response

Message

MDF: Received response from MGW: {0}

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17110 – MDF SPR Message

Message

MDF: {0} - SPR messages: {1}

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17111 – MDF Get Subscriber

Message

MDF: {0} - Query result: {1}

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17112 – MDF Illegal Notify Subscriber**Message**

MDF: Illegal {0}; {1}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17113 – MDF Soap Request**Message**

MDF: SOAP request message: {0}

Description**Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17114 – MDF Soap Response

Message

MDF: SOAP response message: {0}

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17115 – MDF Out SPR Message

Message

MDF: {0} - SPR messages: => {1}

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server
Mediation

Group
Sync

Recovery

1. No action required.

17116 – MDF IMSI Not In SPR

Message
MDF: IMSI(*{0}*) not in SPR IMSI range

Description

Severity
Info

Notification
Trace Log

Alarm
No

Trap
No

Server
Mediation

Group
Sync

Recovery

1. No action required.

17118 – MDF IMSI In SPR

Message
MDF: IMSI(*{0}*) in SPR IMSI range: *{1}*

Description

Severity
Info

Notification
Trace Log

Alarm
No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17119 – MDF IMSI In S-SPR

Message

MDF: IMSI(*{0}*) in S-SPR IMSI range: *{1}*

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17120 – MDF DYQ Was Expired

Message

MDF: Discard expired dynamic quota: *{0}*

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17121 – MDF Quota Was Expired**Message**

MDF: Discard initial quota usage because it based-dynamic-quota was expired: {0}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

Sync

Recovery

1. No action required.

17122 – MDF Deduct Usage Fail**Message**

MDF: Failed to deduct usage ({0}) for {1}: {2}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

QuotaRequest

Recovery

1. No action required.

17123 – MDF Deductible Quotas

Message

MDF: Deductible quotas: {0}

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

QuotaRequest

Recovery

1. No action required.

17124 – MDF Reset For Deduct

Message

MDF: Next reset time arrived, reset quota({0} -> {1}, {2} -> {3}) from {4}.15)({6})

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

QuotaRequest

Recovery

1. No action required.

17125 – MDF Do Deduct Usage**Message**MDF: Deduct quota usage(*{0}* -> *{1}*) from *{2}*.*{3}*(*{4}*)**Description****Severity**

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

Mediation

Group

QuotaRequest

Recovery

1. No action required.

17301 – Clearance Started**Message**Clearance: MPE session clearance will start. Active sessions are *{0}*.

Description

Severity

Always

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

17302 – Clearance Duplicating

Message

Clearance: MPE session clearance has been started.

Description

The MPE session clearance is started.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

17303 – Clearance Abort

Message

Clearance: MPE session clearance transaction is aborted.

Description

The MPE session clearance transaction was aborted.

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

17304 – Clearance Session Terminate**Message**

Clearance: Session {0} will be terminated.

Description**Severity**

Debug

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

17305 – Clearance Finished

Message

Clearance: Task finished, terminate {0} sessions: success {1} and failed {2}.

Description

Severity

Info

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

17306 – KT Reject Invalid Sub

Message

Diameter: Rejecting invalid KT sub-subscriber on session: {0}

Description

Severity

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

17307 – PUA Failure of Reset

Message

SH: Received PUA failure related to quota reset for subscriber: {0}

Description**Severity**

Warning

Notification

Trace Log

Alarm

No

Trap

No

Server

MPE

Group

Diameter

Recovery

1. No action required.

Alarms and Events

This chapter provides general alarm and event information, and lists the types of alarms and events that can occur on the system. Alarms and events are recorded in a database log table.

Note: Alarms for all modes are represented in this list (cable, wireline, and wireless).

Note: If you encounter an alarm not in this document, contact [My Oracle Support](#).

Alarms formatting information

This section of the document provides information to help you understand why an alarm occurred and to provide a recovery procedure to help correct the condition that caused the alarm.

The information provided about each alarm includes:

Alarm Group

The type of alarm that has occurred. For a list of Event types see [Alarm and event types](#).

Description

The reason or cause for the alarm.

Severity

The severity of the alarm. This severity may vary, depending on user-defined and specific application settings.

Instance

HA Score

The HA impact of the alarm: Normal, Failed, or Degraded.

Auto Clear Seconds

The number of seconds required for the alarm to automatically clear (if applicable).

OID

The alarm identifier that appears in SNMP traps.

Alarm ID

The alarm identifier that is used internally (if applicable).

Recovery

Lists any necessary steps for correcting or preventing the alarm.

Alarm and event types

[Table 3-1](#) describes the possible alarm/event types that can be displayed.

Note: Not all applications use all of the alarm types listed.

Table 3-1 Alarm and Event Types

Type Name	Type
APPL	Application
CAF	Communication Agent (ComAgent)
CAPM	Computer-Aided Policy Making (Diameter Mediation)
CFG	Configuration
CHG	Charging
CNG	Congestion Control
COLL	Collection
DAS	Diameter Application Server (Message Copy)
DB	Database
DIAM	Diameter
DISK	Disk
DNS	Domain Name Service
DPS	Data Processor Server
ERA	Event Responder Application
FABR	Full Address Based Resolution
HA	High Availability
HTTP	Hypertext Transfer Protocol
IDIH	Integrated DIH
IF	Interface
IP	Internet Protocol
IPFE	IP Front End
LOADGEN	Load Generator
LOG	Logging
MEAS	Measurements
MEM	Memory
NAT	Network Address Translation

Table 3-1 (Cont.) Alarm and Event Types

Type Name	Type
NP	Number Portability
OAM	Operations, Administration & Maintenance
PCRF	Policy Charging Rules Function
PDRA	Policy Diameter Routing Agent
PLAT	Platform
PROC	Process
PROV	Provisioning
pSBR	Policy SBR
QP	QBus
RBAR	Range-Based Address Resolution
REPL	Replication
SCTP	Stream Control Transmission Protocol
SDS	Subscriber Database Server
SIGC	Signaling Compression
SIP	Session Initiation Protocol Interface
SL	Selective Logging
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack
SW	Software (generic event type)
TCP	Transmission Control Protocol

Alarm and Event Severity Levels

Alarms can be one of three severity levels:

1. Critical
2. Major
3. Minor

Events note the occurrence of an expected condition and are logged in the Trace Log. Events have these severity levels:

1. Emergency
2. Alert
3. Critical

4. Error
5. Warning
6. Notice
7. Info
8. Debug

Platform (31000-32800)

This section provides information and recovery procedures for the Platform alarms, ranging from 31000-32800.

31000 - S/W fault

Alarm Group:

SW

Description:

Program impaired by s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolSwFaultNotify

Recovery:

1. No action is required. This event is used for command-line tool errors only.

31001 - S/W status

Alarm Group:

SW

Description:

Program status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolSwStatusNotify

Recovery:

1. No action required.

31002 - Process watchdog failure

Alarm Group:

SW

Description:

Process watchdog timed out.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolProcWatchdogFailureNotify

Recovery:

1. Alarm indicates a stuck process was automatically recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs ,and it is recommended to contact [My Oracle Support](#).

31003 - Tab thread watchdog failure

Alarm Group:

SW

Description:

Tab thread watchdog timed out

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolThreadWatchdogFailureNotify

Recovery:

1. Alarm indicates a stuck process was automatically recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs, and it is recommended to contact [My Oracle Support](#).

31004 - Test Status

Alarm Type: TEST

Description: For testing purposes only

Severity: Info

OID: comcolTestStatNotify

Recovery:

1. Test message. No action necessary.

31005 - Test Fault

Alarm Type: TEST

Description: For testing purposes only

Severity: Minor

OID: comcolTestFaultNotify

Recovery:

1. Test message. No action necessary.

31100 - Database replication fault

Alarm Group:

SW

Description:

The Database replication process is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.
2. It is recommended to contact [My Oracle Support](#).

31101 - Database replication to slave failure

Alarm Group:

REPL

Description:

Database replication to a slave database has failed. This alarm is generated when:

- The replication master finds the replication link is disconnected from the slave.
- The replication master's link to the replication slave is OOS, or the replication master cannot get the slave's correct HA state because of a failure to communicate.
- The replication mode is relayed in a cluster and either:
 - No nodes are active in cluster, or
 - None of the nodes in cluster are getting replication data.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepToSlaveFailureNotify

Recovery:

1. Verify the path for all services on a node by typing `path.test -a <toNode>` in a command interface to test the paths for all services.
2. Use the path test command to test the communication between nodes by typing `iqd -pE NodeInfo` to get the node ID. Then type `path.test -a <nodeid>` to test the paths for all services.
3. Examine the Platform savelogs on all MPs, SO, and NO by typing `sudo /usr/TKLC/plat/sbin/savelogs_plat` in the command interface. The plat savelogs are in the /tmp directory.
4. Check network connectivity between the affected servers.
5. If there are no issues with network connectivity, contact [My Oracle Support](#).

31102 - Database replication from master failure

Alarm Group:

REPL

Description:

Database replication from a master database has failed. This alarm is generated when the replication slave finds the replication link is disconnected from the master.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepFromMasterFailureNotify

Recovery:

1. Verify the path for all services on a node by typing `path.test -a <toNode>` in a command interface to test the paths for all services.
2. Use the path test command to test the communication between nodes by typing `iqd -pE NodeInfo` to get the node ID. Then type `path.test -a <nodeid>` to test the paths for all services.

3. Examine the Platform savelogs on all MPs, SO, and NO by typing `sudo /usr/TKLC/plat/sbin/savelogs_plat` in the command interface. The plat savelogs are in the /tmp directory.
4. Indicates replication subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
5. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact [My Oracle Support](#).

31103 - DB Replication update fault

Alarm Group:

REPL

Description:

Database replication process cannot apply update to DB.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepUpdateFaultNotify

Recovery:

1. This alarm indicates a transient error occurred within the replication subsystem, but the system has recovered, so no additional steps are needed.
2. If the problem persists, collect savelogs, and it is recommended to contact [My Oracle Support](#).

31104 - DB Replication latency over threshold

Alarm Group:

REPL

Description:

Database replication latency has exceeded thresholds

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepLatencyNotify

Recovery:

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, it is recommended to contact [My Oracle Support](#).

31105 - Database merge fault

Alarm Group:

SW

Description:

The database merge process (inetmerge) is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbMergeFaultNotify

Recovery:

1. This alarm indicates a transient error occurred within the merging subsystem, but the system has recovered, so no additional steps are needed.
2. If the problem persists, collect savelogs, and it is recommended to contact [My Oracle Support](#).

31106 - Database merge to parent failure

Alarm Group:

COLL

Description:

Database merging to the parent Merge Node has failed.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolDbMergeToParentFailureNotify

Recovery:

1. This alarm indicates the merging subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact [My Oracle Support](#).

31107 - Database merge from child failure

Alarm Group:

COLL

Description:

Database merging from a child Source Node has failed.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbMergeFromChildFailureNotify

Recovery:

1. This alarm indicates the merging subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact [My Oracle Support](#).

31108 - Database merge latency over threshold

Alarm Group:

COLL

Description:

Database Merge latency has exceeded thresholds

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbMergeLatencyNotify

Recovery:

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, it is recommended to contact [My Oracle Support](#).

31109 - Topology config error

Alarm Group:

DB

Description:

Topology is configured incorrectly

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolTopErrorNotify

Recovery:

1. This alarm may occur during initial installation and configuration of a server. No action is necessary at that time.
2. If this alarm occurs after successful initial installation and configuration of a server, it is recommended to contact [My Oracle Support](#).

31110 - Database audit fault**Alarm Group:**

SW

Description:

The Database service process (idbsvc) is impaired by a s/w fault.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbAuditFaultNotify

Recovery:

1. Alarm indicates an error occurred within the database audit system, but the system has recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs, and it is recommended to contact [My Oracle Support](#).

31111 - Database merge audit in progress

Alarm Group:

COLL

Description:

Database Merge Audit between mate nodes in progress

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbMergeAuditNotify

Recovery:

1. No action required.

31112 - DB replication update log transfer timed out

Alarm Group:

REPL

Description:

DB Replicated data may not have transferred in the time allotted.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

30

OID:

comcolDbRepUpLogTransTimeoutNotify

Recovery:

1. No action required.
2. It is recommended to contact [My Oracle Support](#) if this occurs frequently.

31113 - DB replication manually disabled

Alarm Group:

REPL

Description:

DB Replication Manually Disabled

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolDbReplicationManuallyDisabledNotify

Recovery:

1. No action required.

31114 - DB replication over SOAP has failed

Alarm Group:

REPL

Description:

Database replication of configuration data via SOAP has failed.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

3600

OID:

comcolDbReplicationSoapFaultNotify

Recovery:

1. This alarm indicates a SOAP subsystem is unable to connect to a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact [My Oracle Support](#).

31115 - Database service fault

Alarm Group:

SW

Description:

The Database service process (idbsvc) is impaired by a s/w fault.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbServiceFaultNotify

Recovery:

1. Alarm indicates an error occurred within the database disk service subsystem, but the system has recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs, and it is recommended to contact [My Oracle Support](#).

31116 - Excessive shared memory

Alarm Group:

MEM

Description:

The amount of shared memory consumed exceeds configured thresholds.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolExcessiveSharedMemoryConsumptionNotify

Recovery:

1. This alarm indicates that a server has exceeded the engineered limit for shared memory usage and there is a risk that application software will fail. Because there is no automatic recovery for this condition, it is recommended to contact [My Oracle Support](#).

31117 - Low disk free**Alarm Group:**

DISK

Description:

The amount of free disk is below configured thresholds

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolLowDiskFreeNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, it is recommended to contact [My Oracle Support](#).

31118 - Database disk store fault**Alarm Group:**

DISK

Description:

Writing the database to disk failed

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbDiskStoreFaultNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, it is recommended to contact [My Oracle Support](#).

31119 - Database updatelog overrun

Alarm Group:

DB

Description:

The Database update log was overrun increasing risk of data loss

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbUpdateLogOverrunNotify

Recovery:

1. This alarm indicates a replication audit transfer took too long to complete and the incoming update rate exceeded the engineered size of the update log. The system will automatically retry the audit, and if successful, the alarm will clear and no further recovery steps are needed.
2. If the alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31120 - Database updatelog write fault

Alarm Group:

DB

Description:

A Database change cannot be stored in the updatelog

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbUpdateLogWriteFaultNotify

Recovery:

1. This alarm indicates an error has occurred within the database update log subsystem, but the system has recovered.
2. If the alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31121 - Low disk free early warning

Alarm Group:

DISK

Description:

The amount of free disk is below configured early warning thresholds

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolLowDiskFreeEarlyWarningNotify

Recovery:

1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
2. If there are no files known to be unneeded, it is recommended to contact [My Oracle Support](#).

31122 - Excessive shared memory early warning

Alarm Group:

MEM

Description:

The amount of shared memory consumed exceeds configured early warning thresholds

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

1. This alarm indicates that a server is close to exceeding the engineered limit for shared memory usage and the application software is at risk to fail. There is no automatic recovery or recovery steps.
2. It is recommended to contact [My Oracle Support](#).

31123 - Database replication audit command complete

Alarm Group:

REPL

Description:

ADIC found one or more errors that are not automatically fixable.

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepAuditCmdCompleteNotify

Recovery:

1. No action required.

31124 - ADIC error**Alarm Group:**

REPL

Description:

An ADIC detected errors

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepAuditCmdErrNotify

Recovery:

1. It is recommended to contact [My Oracle Support](#).

31125 - Database durability degraded**Alarm Group:**

REPL

Description:

Database durability has dropped below configured durability level

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbDurabilityDegradedNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31126 - Audit blocked

Alarm Group:

REPL

Description:

Site Audit Controls blocked an inter-site replication audit due to the number in progress per configuration.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolAuditBlockedNotify

Recovery:

1. This alarm indicates that WAN network usage has been limited following a site recovery. No recovery action is needed.

31127 - DB Replication Audit Complete

Alarm Group:

REPL

Description:

DB replication audit completed

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbRepAuditCompleteNotify

Recovery:

1. No action required.

31128 - ADIC Found Error

Alarm Group:

REPL

Description:

ADIC found one or more errors that are not automatically fixable.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbADICErrorNotify

Recovery:

1. This alarm indicates a data integrity error was found by the background database audit mechanism, and there is no automatic recovery.
2. It is recommended to contact [My Oracle Support](#).

31129 - ADIC Found Minor Issue

Alarm Group:

REPL

Description:

ADIC found one or more minor issues that can most likely be ignored

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

14400

OID:

comcolDbADICWarn

Recovery:

1. No action required.

31130 - Network health warning

Alarm Group:

NET

Description:

Network health issue detected

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolNetworkHealthWarningNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31131 - DB Ousted Throttle Behind

Alarm Group:

DB

Description:

DB ousted throttle may be affecting processes.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolOustedThrottleWarnNotify

Recovery:

1. This alarm indicates that a process has failed to release database memory segments which is preventing new replication audits from taking place. There is no automatic recovery for this failure.
2. Run 'procsh -o' to identify involved processes.
3. It is recommended to contact [My Oracle Support](#).

31132 - DB Replication Precedence Relaxed

Event Type

REPL

Description

Standby Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Databases to update as fast as possible.

Severity

Info

Instance

Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score

Normal

Throttle Seconds

150

OID

comcolDbRepPrecRelaxedNotify

Recovery

1. No action required.

31133 - DB Replication Switchover Exceeds Threshold

Alarm Group

REPL

Description

DB Replication Active to Standby switchover exceeded maximum switchover time.

Severity

Major

Instance

Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score

Normal

Auto Clear Seconds

300

OID

comcolDbRepSwitchoverNotify

Recovery

1. If this alarm is raised, it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31134 - DB Site Replication To Slave Failure

Alarm Group

REPL

Description

DB Site replication to a slave DB has failed.

Severity

Minor

Instance

Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score

Normal

Auto Clear Seconds

300

OID

comcolDbSiteRepToSlaveFailureNotify

Recovery

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31135 - DB Site Replication From Master Failure**Alarm Group**

REPL

Description

DB Site replication from a master DB has failed.

Severity

Minor

Instance

Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score

Normal

Auto Clear Seconds

300

OID

comcolDbSiteRepFromMasterFailureNotify

Recovery

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31136 - DB Site Replication Precedence Relaxed**Event Type**

REPL

Description

Standby Site Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Site Databases to update as fast as possible.

Severity

Info

Instance

Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score

Normal

Throttle Seconds

150

OID

comcolDbSiteRepPrecRelaxedNotify

Recovery

1. No action required.

31137 - DB Site Replication Latency Over Threshold

Alarm Group

REPL

Description

DB Site Replication latency has exceeded thresholds.

Severity

Major

Instance

Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score

Normal

Auto Clear Seconds

300

OID

comcolDbSiteRepLatencyNotify

Recovery

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, it is recommended to contact [My Oracle Support](#).

31140 - Database perl fault

Alarm Group:

SW

Description:

Perl interface to Database is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbPerlFaultNotify

Recovery:

1. This alarm indicates an error has occurred within a Perl script, but the system has recovered.
2. If the alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31145 - Database SQL fault

Alarm Group:

SW

Description:

SQL interface to Database is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbSQLFaultNotify

Recovery:

1. This alarm indicates an error has occurred within the MySQL subsystem, but the system has recovered.
2. If this alarm occurs frequently, it is recommended to collect savelogs and contact [My Oracle Support](#).

31146 - DB mastership fault

Alarm Group:

SW

Description:

DB replication is impaired due to no mastering process (inetrep/inetrep).

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. It is recommended to contact [My Oracle Support](#).

31147 - DB upsynclog overrun

Alarm Group:

SW

Description:

UpSyncLog is not big enough for (WAN) replication.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbUpSyncLogOverrunNotify

Recovery:

1. This alarm indicates that an error occurred within the database replication subsystem. A replication audit transfer took too long to complete, and during the audit the incoming update rate exceeded the engineered size of the update log. The replication subsystem will automatically retry the audit, and if successful, the alarm will clear.
2. If the alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31148 - DB lock error detected

Alarm Group:

DB

Description:

The DB service process (idbsvc) has detected an IDB lock-related error caused by another process. The alarm likely indicates a DB lock-related programming error, or it could be a side effect of a process crash.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolDbLockErrorNotify

Recovery:

1. This alarm indicates an error occurred within the database disk service subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31200 - Process management fault

Alarm Group:

SW

Description:

The process manager (procmgr) is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolProcMgmtFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31201 - Process not running

Alarm Group:

PROC

Description:

A managed process cannot be started or has unexpectedly terminated

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolProcNotRunningNotify

Recovery:

1. This alarm indicates that the managed process exited unexpectedly due to a memory fault, but the process was automatically restarted.
2. It is recommended to collect savelogs and contact [My Oracle Support](#).

31202 - Unkillable zombie process

Alarm Group:

PROC

Description:

A zombie process exists that cannot be killed by procmgr. procmgr will no longer manage this process.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolProcZombieProcessNotify

Recovery:

1. This alarm indicates managed process exited unexpectedly and was unable to be restarted automatically.
2. It is recommended to collect savelogs and contact [My Oracle Support](#).

31206 - Process mgmt monitoring fault

Alarm Group:

SW

Description:

The process manager monitor (pm.watchdog) is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolProcMgmtMonFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.

2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31207 - Process resource monitoring fault

Alarm Group:

SW

Description:

The process resource monitor (ProcWatch) is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolProcResourceMonFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process monitoring subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31208 - IP port server fault

Alarm Group:

SW

Description:

The run environment port mapper (re.portmap) is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:
comcolPortServerFaultNotify

Recovery:

1. This alarm indicates an error occurred within the port mapping subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31209 - Hostname lookup failed

Alarm Group:
SW

Description:
Unable to resolve a hostname specified in the NodeInfo table

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHostLookupFailedNotify

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31213 - Process scheduler fault

Alarm Group:
SW

Description:
The process scheduler (ProcSched/runat) is impaired by a s/w fault

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolProcSchedulerFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31214 - Scheduled process fault

Alarm Group:

PROC

Description:

A scheduled process cannot be executed or abnormally terminated

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolScheduleProcessFaultNotify

Recovery:

1. This alarm indicates that a managed process exited unexpectedly due to a memory fault, but the system has recovered.
2. It is recommended to contact [My Oracle Support](#).

31215 - Process resources exceeded

Alarm Group:

SW

Description:

A process is consuming excessive system resources.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

14400

OID:

comcolProcResourcesExceededFaultNotify

Recovery:

1. This alarm indicates a process has exceeded the engineered limit for heap usage and there is a risk the application software will fail.
2. Because there is no automatic recovery for this condition, it is recommended to contact [My Oracle Support](#).

31216 - SysMetric configuration error**Alarm Group:**

SW

Description:

A SysMetric Configuration table contains invalid data

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolSysMetricConfigErrorNotify

Recovery:

1. This alarm indicates a system metric is configured incorrectly.
2. It is recommended to contact [My Oracle Support](#).

31217 - Network Health Warning

Alarm Group

SW

Description

Missed Heartbeats Detected

Severity

Minor

Instance

IP Address

HA Score

Normal

Auto Clear Seconds

300

OID

comcolNetworkHealthWarningNotify

Recovery

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31220 - HA configuration monitor fault

Alarm Group:

SW

Description:

The HA configuration monitor is impaired by a s/w fault.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaCfgMonitorFaultNotify

Recovery:

1. It is recommended to contact [My Oracle Support](#).

31221 - HA alarm monitor fault

Alarm Group:

SW

Description:

The high availability alarm monitor is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaAlarmMonitorFaultNotify

Recovery:

1. It is recommended to contact [My Oracle Support](#).

31222 - HA not configured

Alarm Group:

HA

Description:

High availability is disabled due to system configuration

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaNotConfiguredNotify

Recovery:

1. It is recommended to contact [My Oracle Support](#).

31223 - HA Heartbeat transmit failure

Alarm Group:

HA

Description:

The high availability monitor failed to send heartbeat.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaHbTransmitFailureNotify

Recovery:

1. This alarm clears automatically when the server successfully registers for HA heartbeating.
2. If this alarm does not clear after a couple minutes, it is recommended to contact [My Oracle Support](#).

31224 - HA configuration error

Alarm Group:

HA

Description:

High availability configuration error

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaCfgErrorNotify

Recovery:

1. This alarm indicates a platform configuration error in the High Availability or VIP management subsystem.
2. Because there is no automatic recovery for this condition, it is recommended to contact [My Oracle Support](#).

31225 - HA service start failure**Alarm Group:**

HA

Description:

The required high availability resource failed to start.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0

OID:

comcolHaSvcStartFailureNotify

Recovery:

1. This alarm clears automatically when the HA daemon is successfully started.
2. If this alarm does not clear after a couple minutes, it is recommended to contact [My Oracle Support](#).

31226 - HA availability status degraded**Alarm Group:**

HA

Description:

The high availability status is degraded due to raised alarms.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0

OID:

comcolHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, it is recommended to contact [My Oracle Support](#).

31227 - HA availability status failed

Alarm Group:

HA

Description:

The high availability status is failed due to raised alarms.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

N/A

OID:

comcolHaAvailFailedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, it is recommended to contact [My Oracle Support](#).

31228 - HA standby offline

Alarm Group:

HA

Description:

High availability standby server is offline.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolHaStandbyOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, it is recommended to look for network connectivity issues and/or contact [My Oracle Support](#).

31229 - HA score changed**Alarm Group:**

HA

Description:

High availability health score changed

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaScoreChangeNotify

Recovery:

1. Status message - no action required.

31230 - Recent alarm processing fault

Alarm Group:
SW

Description:
The recent alarm event manager (raclerk) is impaired by a s/w fault.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolRecAlarmEvProcFaultNotify

Recovery:

1. This alarm indicates an error occurred within the alarm management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31231 - Platform alarm agent fault

Alarm Group:
SW

Description:
The platform alarm agent impaired by a s/w fault

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolPlatAlarmAgentNotify

Recovery:

1. This alarm indicates an error occurred within the alarm management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact [My Oracle Support](#).

31232 - Late heartbeat warning

Alarm Group:
HA

Description:
High availability server has not received a message on specified path within the configured interval.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaLateHeartbeatWarningNotify

Recovery:

1. No action is required. This is a warning and can be due to transient conditions. If there continues to be no heartbeat from the server, alarm [31228 - HA standby offline](#) occurs.

31233 - HA Path Down

Alarm Group:
HA

Description:
High availability path loss of connectivity

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaPathDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the secondary path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues on the secondary network.
3. It is recommended to contact [My Oracle Support](#).

31234 - Untrusted Time Upon Initialization

Alarm Group:

REPL

Description:

Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery will often will require rebooting the server.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolUtrustedTimeOnInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31235 - Untrusted Time After Initialization

Alarm Group:

REPL

Description:

After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, etc. There are often accompanying Platform alarms to guide correction. Generally, applications remain running, but time-stamped data is likely incorrect, reports may be negatively affected, some behavior may be improper, etc.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolUtrustedTimePostInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

31236 - HA Link Down

Alarm Group:

HA

Description:

High availability TCP link is down.

Severity:

Critical

Instance:

Remote node being connected to plus the path identifier

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaLinkDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the specified path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, it is recommended to look for network connectivity issues on the primary network and/or contact [My Oracle Support](#).

31240 - Measurements collection fault

Alarm Group:

SW

Description:

The measurements collector (statclerk) is impaired by a s/w fault.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolMeasCollectorFaultNotify

Recovery:

1. This alarm indicates that an error within the measurement subsystem has occurred, but that the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to collect savelogs and contact [My Oracle Support](#).

31250 - RE port mapping fault

Alarm Group:

SW

Description:

The IP service port mapper (re.portmap) is impaired by a s/w fault

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolRePortMappingFaultNotify

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.

31260 - SNMP Agent

Alarm Group:

SW

Description:

The SNMP agent (cmsnmpa) is impaired by a s/w fault.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

eagleXgDsrDbcomcolSnmpAgentNotify

Recovery:

1. This alarm indicates an error occurred within the SNMP subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to collect savelogs and contact [My Oracle Support](#).

31261 - SNMP Configuration Error

Alarm Group

SW

Description

A SNMP configuration error was detected

Severity

Minor

Instance

comcolAlarmSrcNode, comcolAlarmNumber, comcolAlarmInstance, comcolAlarmSeverity, comcolAlarmText, comcolAlarmInfo, comcolAlarmGroup, comcolServerHostname, comcolAlarmSequence, comcolAlarmTimestamp, comcolAlarmEventType, comcolAlarmProbableCause, comcolAlarmAdditionalInfo

HA Score

Normal

Auto Clear Seconds

0 (zero)

OID

comcolSnmpConfigNotify

Recovery

1. Export event history for the given server and all processes.
2. It is recommended to contact [My Oracle Support](#) for assistance.

31270 - Logging output

Alarm Group:

SW

Description:

Logging output set to Above Normal

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolLoggingOutputNotify

Recovery:

1. Extra diagnostic logs are being collected, potentially degrading system performance. Turn off the debugging log.

31280 - HA Active to Standby transition

Alarm Group:

HA

Description:

HA active to standby activity transition

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, it is recommended to contact [My Oracle Support](#).

31281 - HA Standby to Active transition

Alarm Group:

HA

Description:

HA standby to active activity transition

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolStandbyToActiveTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, it is recommended to contact [My Oracle Support](#).

31282 - HA Management Fault

Alarm Group:

HA

Description:

The HA manager (cmha) is impaired by a software fault.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaMgmtFaultNotify

Recovery:

1. This alarm indicates an error occurred within the High Availability subsystem, but the system has automatically recovered.
2. If the alarm occurs frequently, it is recommended to contact [My Oracle Support](#).

31283 - Lost Communication with server

Alarm Group:

HA

Description:

Highly available server failed to receive mate heartbeats

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

comcolHaServerOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues and/or it is recommended to contact [My Oracle Support](#) for assistance.

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Group:

HA

Description:

High availability remote subscriber has not received a heartbeat within the configured interval.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaRemoteHeartbeatWarningNotify

Recovery:

1. No action required. This is a warning and can be due to transient conditions. The remote subscriber will move to another server in the cluster.
2. If there continues to be no heartbeat from the server, it is recommended to contact [My Oracle Support](#).

31285 - HA Node Join Recovery Entry

Alarm Group:

HA

Description:

High availability node join recovery entered

Severity:

Info

Instance:

Cluster set key of the DC outputting the event

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaSbrEntryNotify

Recovery:

1. No action required; this is a status message generated when one or more unaccounted for nodes join the designated coordinators group.

31286 - HA Node Join Recovery Plan

Alarm Group:

HA

Description:

High availability node join recovery plan

Severity:

Info

Instance:

Names of HA Policies (as defined in HA policy configuration)

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaSbrPlanNotify

Recovery:

1. No action required; this is a status message output when the designated coordinator generates a new action plan during node join recovery.

31287 - HA Node Join Recovery Complete

Alarm Group:

HA

Description:

High availability node join recovery complete

Severity:

Info

Instance:

Names of HA Policies (as defined in HA policy configuration)

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaSbrCompleteNotify

Recovery:

1. No action required; this is a status message output when the designated coordinator finishes running an action plan during node join recovery.

31288 - HA Site Configuration Error

Alarm Group

HA

Description

High availability site configuration error

Severity

Critical

Instance

GroupName, Policy ID, Site Name

HA Score

Normal

Auto Clear Seconds

0 (zero)

OID

comcolHaBadSiteCfgNotify

Recovery

1. If this alarm does not clear after correcting the configuration, it is recommended to contact [My Oracle Support](#) for assistance.

31290 - HA Process Status

Alarm Group:

HA

Description:

HA manager (cmha) status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaProcessStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31291 - HA Election Status

Alarm Group:

HA

Description:

HA DC Election status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaElectionStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31292 - HA Policy Status

Alarm Group:

HA

Description:

HA Policy plan status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaPolicyStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31293 - HA Resource Link Status

Alarm Group:

HA

Description:

This alarm is raised for nodes in our topology that we should be connected to (i.e., not OOS), but that we do not have any TCP links to it over any configured paths. It does not matter why the links were not established (networking connectivity, node not running, etc.).

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaRaLinkStatusNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored. It clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues.

3. If the problem persists, it is recommended to contact [My Oracle Support](#).

31294 - HA Resource Status

Alarm Group:

HA

Description:

HA Resource registration status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaResourceStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31295 - HA Action Status

Alarm Group:

HA

Description:

HA Resource action status

Severity:

Info

Instance

N/A

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaActionStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31296 - HA Monitor Status

Alarm Group:

HA

Description:

HA Monitor action status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaMonitorStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31297 - HA Resource Agent Info

Alarm Group:

HA

Description:

HA Resource Agent Info

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaRaInfoNotify

Recovery:

1. This event is used for internal logging. No action is required.

31298 - HA Resource Agent Detail

Alarm Group:

HA

Description:

Resource Agent application detailed information

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaRaDetailNotify

Recovery:

1. This event is used for internal logging. No action is required.

31299 - HA Notification Status

Alarm Group:

HA

Description:

HA Notification status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaNotificationNotify

Recovery:

1. No action required.

31300 - HA Control Status

Alarm Group:

HA

Description:

HA Control action status

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

300

OID:

comcolHaControlNotify

Recovery:

1. No action required.

31301 - HA Topology Events

Alarm Group:

HA

Description:

HA Topology events

Severity:

Info

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

eagleXgDsrHaTopologyNotify

Recovery:

1. No action required.

31322 - HA Configuration Error

Alarm Group

HA

Description

High availability configuration error

Severity

Minor

Instance

NodeID, or HA Tunnel ID

HA Score

Normal

Auto Clear Seconds

0 (zero)

OID

comcolHaBadCfgNotify

Recovery

1. It is recommended to contact [#unique_943](#).

32100 - Breaker Panel Feed Unavailable

Alarm Group:

PLAT

Description:

Breaker Panel Breaker Unavailable

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdBrkPnlFeedUnavailable

Recovery:

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Group:

PLAT

Description:

Breaker Panel Breaker Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdBrkPnlBreakerFailure

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

Alarm Group: PLAT

Description: Breaker Panel Monitoring Failure

Severity: Critical

Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdBrkPnlMntFailureNotify

Recovery

1. Contact [My Oracle Support](#) to request hardware replacement.

32103 - Power Feed Unavailable

Alarm Group:

PLAT

Description:

Power Feed Unavailable

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPowerFeedUnavail

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Group:

PLAT

Description:

Power Supply 1 Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPowerSupply1Failure

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Group:

PLAT

Description:

Power Supply 2 Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPowerSupply2Failure

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group: PLAT

Description: Power Supply 3 Failure

Severity: Critical

Instance: May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score: Normal

Auto Clear Seconds: 0 (zero)

OID: tpdPowerSupply3FailureNotify

Recovery

1. Contact [My Oracle Support](#) to request hardware replacement.

32107 - Raid Feed Unavailable

Alarm Group:

PLAT

Description:

Raid Feed Unavailable

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdRaidFeedUnavailable

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Group:

PLAT

Description:

Raid Power 1 Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdRaidPower1Failure

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Group:

PLAT

Description:

Raid Power 2 Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdRaidPower2Failure

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Group:

PLAT

Description:

Raid Power 3 Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdRaidPower3Failure

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32111 - Device Failure

Alarm Group:

PLAT

Description:

Device Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDeviceFailure

Recovery:

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32112 - Device Interface Failure

Alarm Group:

PLAT

Description:

Device Interface Failure

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDeviceIfFailure

Recovery:

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32113 - Uncorrectable ECC memory error

Alarm Group:

PLAT

Description:

This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdEccUncorrectableError

Alarm ID:

TKSPLATCR14

Recovery:

1. Contact the hardware vendor to request hardware replacement.

32114 - SNMP get failure

Alarm Group:

PLAT

Description:

The server failed to receive SNMP information from the switch.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSNMPGetFailure

Alarm ID:

TKSPLATCR15

Recovery:

1. Verify device is active and responds to the ping command.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

32115 - TPD NTP Daemon Not Synchronized Failure

Alarm Group:

PLAT

Description:

This alarm indicates the server's current time precedes the timestamp of the last known time the servers time was good.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdNTPDaemonNotSynchronizedFailure

Alarm ID:

TKSPLATCR16

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
 - a. Ensure ntpd service is running with correct options: -x -g.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Type `/usr/sbin/ntpd -c sysinfo` to check the current state of the ntpd daemon.
 - d. Verify the ntp peer configuration; execute `ntpq -np`; and analyze the output. Verify peer data, such as tally code (first column before remote), remote, refid, stratum (st), and jitter, are valid for server.
 - e. Execute `ntpstat` to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server, then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, then restart the ntpd service.
3. If problem persists, then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. Reset ntpd:
 - `sudo service ntpd stop`

- `sudo ntpdate <ntp server ip>`
 - `sudo service ntpd start`
4. Conform to recommended NTP topology and strategy.
 - No fewer than three references are recommended.
 - If selecting a different number, the number should be odd.
 - No intermediate reference should be a virtualized server.
 - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
 5. If the problem persists, it is recommended to contact [My Oracle Support](#).

32116 - TPD Server's Time Has Gone Backwards

Alarm Group:

PLAT

Description:

This alarm indicates the server's current time precedes the timestamp of the last known time the server's time was good.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdNTPTimeGoneBackwards

Alarm ID:

TKSPLATCR17

Recovery:

1. Verify NTP settings and NTP sources are providing accurate time.
 - a. Ensure ntpd service is running with correct options: `-x -g`
 - b. Verify the content of the `/etc/ntp.conf` file is correct for the server.
 - c. Type `/usr/sbin/ntpdc -c sysinfo` to check the current state of the ntpd daemon.

- d. Verify the ntp peer configuration; execute `ntpq -p`; and analyze the output. Verify peer data, such as tally code (first column before remote), remote, refid, stratum (st), and jitter, are valid for server.
 - e. Execute `ntpstat` to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server, then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, then restart the ntpd service.
 3. If problem persists, then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. Reset ntpd:
 - `sudo service ntpd stop`
 - `sudo ntpdate <ntp server ip>`
 - `sudo service ntpd start`
4. Conform to recommended NTP topology and strategy.
 - No fewer than tree references are recommended.
 - If selecting a different number, the number should be odd.
 - No intermediate reference should be a virtualized server.
 - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact [My Oracle Support](#).

32117 - TPD NTP Offset Check Failure

Alarm Group:

PLAT

Description:

This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

ntpOffsetCheckFailure

Alarm ID:

TKSPLATCR18

Recovery:

1. Verify NTP settings and NTP sources can be reached.
 - a. Ensure ntpd service is running using `ps -ef | grep` or `service ntpd status`.
 - b. Verify the content of the `/etc/ntp.conf` file is correct for the server.
 - c. Type `/usr/sbin/ntpdc -c sysinfo` to check the current state of the ntpd daemon.
 - d. Verify the ntp peer configuration; execute `ntpq -p`; and analyze the output. Verify peer data, such as tally code (first column before remote), remote, refid, stratum (st), and jitter, are valid for server.
 - e. Execute `ntpstat` to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server, then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, then restart the ntpd service.
3. If problem persists, then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - `sudo service ntpd stop`
 - `sudo ntpdate <ntp server ip>`
 - `sudo service ntpd start`
4. Conform to recommended NTP topology and strategy.
 - No fewer than three references are recommended.
 - If selecting a different number, the number should be odd.
 - No intermediate reference should be a virtualized server.
 - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact [My Oracle Support](#).

32300 - Server fan failure

Alarm Group:

PLAT

Description:

This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdFanError

Alarm ID:

TKSPLATMA1

Recovery:

1. Run Syscheck in Verbose mode to determine which server fan assemblies is failing and replace the fan assembly.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

32301 - Server internal disk error

Alarm Group:

PLAT

Description:

This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdIntDiskError

Alarm ID:

TKSPLATMA2

Recovery:

1. Run syscheck in verbose mode.
2. Determine the raid state of the mirrored disks, collect data:

```
cat /proc/mdstat  
cat /etc/raidtab
```
3. It is recommended to contact [My Oracle Support](#) and provide the system health check output and collected data.

32302 - Server RAID disk error**Alarm Group:**

PLAT

Description:

This alarm indicates that the offboard storage server had a problem with its hardware disks.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdRaidDiskError

Alarm ID:

TKSPLATMA3

Recovery

1. It is recommended to contact [My Oracle Support](#).

32303 - Server Platform error

Alarm Group:

PLAT

Description:

This alarm indicates an error such as a corrupt system configuration or missing files.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPlatformError

Alarm ID:

TKSPLATMA4

Recovery:

1. Run syscheck in verbose mode.
2. Determine the raid state of the mirrored disks, collect data:

```
cat /proc/mdstatcat /etc/raidtab
```

3. It is recommended to contact [My Oracle Support](#) and provide the system health check output and collected data.

32304 - Server file system error

Alarm Group:

PLAT

Description:

This alarm indicates unsuccessful writing to at least one of the server's file systems.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:
tpdFileSystemError

Alarm ID:
TKSPLATMA5

Recovery:

1. Run syscheck in verbose mode.
2. Address full file systems identified in syscheck output, and run syscheck in verbose mode.
3. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32305 - Server Platform process error

Alarm Group:
PLAT

Description:
This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPlatProcessError

Alarm ID:
TKSPLATMA6

Recovery:

1. Rerun syscheck in verbose mode.
2. If the alarm has been cleared then the problem is solved.
3. If the alarm has not been cleared then determine the run level of the system.
4. If system run level is not 4 then determine why the system is operating at that run level.

5. If system run level is 4, determine why the required number of instances process(es) are not running.
6. If the alarm persists, it is recommended to contact [My Oracle Support](#) and provide the system health check output.

32306 - Server RAM shortage error

Alarm Group:
PLAT

Description:
Not Implemented.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRamShortageError

Recovery

1. It is recommended to contact [My Oracle Support](#).

32307 - Server swap space shortage failure

Alarm Group:
PLAT

Description:
This alarm indicates that the server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSwapSpaceShortageError

Alarm ID:

TKSPLATMA8

Recovery:

1. Run syscheck in verbose mode.
2. Determine processes using swap.

Note: One method to determine the amount of swap being used by process is:
`grep VmSwap /proc/<process id>/status`

3. It is recommended to contact [My Oracle Support](#) and provide the system health check output and process swap usage.

32308 - Server provisioning network error

Alarm Group:

PLAT

Description:

This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdProvNetworkError

Alarm ID:

TKSPLATMA9

Recovery:

1. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.

2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.
4. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, it is recommended to contact [My Oracle Support](#).

32309 - Eagle Network A Error

Alarm Group:

PLAT

Description:

Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdEagleNetworkAError

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32310 - Eagle Network B Error

Alarm Group:

PLAT

Description:

Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdEagleNetworkBError

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32311 - Sync Network Error

Alarm Group:

PLAT

Description:

Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:

Critical

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSyncNetworkError

Recovery

1. It is recommended to contact [My Oracle Support](#) to request hardware replacement.

32312 - Server disk space shortage error

Alarm Group:

PLAT

Description:

This alarm indicates that one of the following conditions has occurred:

- A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system.

- More than 90% of the total number of available files have been allocated on the file system.
- A file system has a different number of blocks than it had when installed.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDiskSpaceShortageError

Alarm ID:

TKSPLATMA13

Recovery:

1. Run syscheck in verbose mode.
2. Examine contents of identified volume in syscheck output to determine if any large files are in the file system. Delete unnecessary files, or move files off of server. Capture output from "du -sx <file system>".
3. Capture output from "df -h" and "df -i" commands.
4. Determine processes using the file system(s) that have exceeded the threshold.
5. It is recommended to contact [My Oracle Support](#) and provide the system health check output and provide additional file system output.

32313 - Server default route network error

Alarm Group:

PLAT

Description:

This alarm indicates that the default network route of the server is experiencing a problem.

Caution: When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDefaultRouteNetworkError

Recovery:

1. Run syscheck in verbose mode.
2. If the syscheck output is: The default router at <IP_address> cannot be pinged, the router may be down or unreachable. Do the following:
 - a. Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
 - b. Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
 - c. Check with the router administrator to verify that the router is configured to reply to pings on that interface.
 - d. Rerun syscheck.
 - e. If the alarm has not been cleared, it is recommended to collect the syscheck output and contact [My Oracle Support](#).
3. If the syscheck output is: The default route is not on the provisioning network, it is recommended to collect the syscheck output and contact [My Oracle Support](#).
4. If the syscheck output is: An active route cannot be found for a configured default route, it is recommended to collect the syscheck output and contact [My Oracle Support](#).

32314 - Server temperature error

Alarm Group:

PLAT

Description:

The internal temperature within the server is unacceptably high.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdServerTemperatureError

Alarm ID:

TKSPLATMA15

Recovery:

1. Ensure that nothing is blocking the fan intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Run syscheck.
 - a. If the alarm has been cleared, the problem is resolved.
 - b. If the alarm has not been cleared, continue troubleshooting.
4. Replace the filter.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

5. Re-run syscheck.
 - a. If the alarm has been cleared, the problem is resolved.
 - b. If the alarm has not been cleared, continue troubleshooting.
6. If the problem has not been resolved, it is recommended to contact [My Oracle Support](#).

32315 - Server mainboard voltage error

Alarm Group:

PLAT

Description:

This alarm indicates that one or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdServerMainboardVoltageError

Alarm ID:

TKSPLATMA16

Recovery:

1. Run syscheck in verbose mode.
2. If the alarm persists, it is recommended to contact [My Oracle Support](#) and provide the system health check output.

32316 - Server power feed error

Alarm Group:

PLAT

Description:

This alarm indicates that one of the power feeds to the server has failed. If this alarm occurs in conjunction with any Breaker Panel alarm, there might be a problem with the breaker panel.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPowerFeedError

Alarm ID:

TKSPLATMA17

Recovery:

1. Verify that all the server power feed cables to the server that is reporting the error are securely connected.
2. Check to see if the alarm has cleared
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, continue with the next step.
3. Follow the power feed to its connection on the power source. Ensure that the power source is ON and that the power feed is properly secured.
4. Check to see if the alarm has cleared
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, continue with the next step.
5. If the power source is functioning properly and the wires are all secure, have an electrician check the voltage on the power feed.
6. Check to see if the alarm has cleared
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, continue with the next step.
7. If the problem has not been resolved, it is recommended to contact [My Oracle Support](#).

32317 - Server disk health test error

Alarm Group:

PLAT

Description:

Either the hard drive has failed or failure is imminent.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:
tpdDiskHealthError

Alarm ID:
TKSPLATMA18

Recovery:

1. Run syscheck in verbose mode.
2. Replace the hard drives that have failed or are failing.
3. Re-run syscheck in verbose mode.
4. Perform the recovery procedures for the other alarms that may accompany this alarm.
5. If the problem has not been resolved, it is recommended to contact [My Oracle Support](#) and provide the system health check output. .

32318 - Server disk unavailable error

Alarm Group:
PLAT

Description:
The smartd service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskUnavailableError

Alarm ID:
TKSPLATMA19

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32319 - Device error

Alarm Group:

PLAT

Description:

This alarm indicates that the offboard storage server had a problem with its disk volume filling up.

Severity:

Major

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDeviceError

Alarm ID:

TKSPLATMA20

Recovery

1. It is recommended to contact the [My Oracle Support](#).

32320 - Device interface error

Alarm Group:

PLAT

Description:

This alarm indicates that the IP bond is either not configured or down.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDeviceIfError

Alarm ID:

TKSPLATMA21

Recovery:

1. Run syscheck in verbose mode.
2. Investigate the failed bond, and slave devices, configuration:
 - a. Navigate to `/etc/sysconfig/network-scripts` for the persistent configuration of a device.
3. Determine if the failed bond, and slave devices, has been administratively shut down or has operational issues:
 - a. `cat /proc/net/bonding/bondX`, where X is bond designation
 - b. `ethtool <slave device>`
4. If bond, and slaves, are healthy attempt to administratively bring bond up:
 - a. `ifup bondX`
5. If the problem has not been resolved, it is recommended to contact [My Oracle Support](#) and provide the system health check output and the output of the above investigation.

32321 - Correctable ECC memory error

Alarm Group:

PLAT

Description:

This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdEccCorrectableError

Alarm ID:

TKSPLATMA22

Recovery:

1. No recovery necessary.
2. If the condition persists, verify the server firmware. Update the firmware if necessary, and re-run syscheck in verbose mode. Otherwise if the condition persists

and the firmware is up to date, contact the hardware vendor to request hardware replacement.

32322 - Power Supply A error

Alarm Group:

PLAT

Description:

This alarm indicates that power supply 1 (feed A) has failed.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPowerSupply1Error

Alarm ID:

TKSPLATMA23

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. Run syscheck in verbose mode. The output will provide details about what is wrong with the power supply.
3. If the problem persists, it is recommended to contact [My Oracle Support](#) and provide the syscheck verbose output. Power supply 1 (feed A) will probably need to be replaced.

32323 - Power Supply B error

Alarm Group:

PLAT

Description:

This alarm indicates that power supply 2 (feed B) has failed.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdPowerSupply2Error

Alarm ID:

TKSPLATMA24

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. Run syscheck in verbose mode. The output will provide details about what is wrong with the power supply.
3. If the problem persists, it is recommended to contact [My Oracle Support](#) and provide the syscheck verbose output. Power supply 2 (feed B) will probably need to be replaced.

32324 - Breaker panel feed error**Alarm Group:**

PLAT

Description:

This alarm indicates that the server is not receiving information from the breaker panel relays.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdBrkPnlFeedError

Alarm ID:

TKSPLATMA25

Recovery:

1. Verify that the same alarm is displayed by multiple servers:

- If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.
 3. If the problem has not been resolved, it is recommended to contact [My Oracle Support](#) to request that the breaker panel be replaced.

32325 - Breaker panel breaker error

Alarm Group:

PLAT

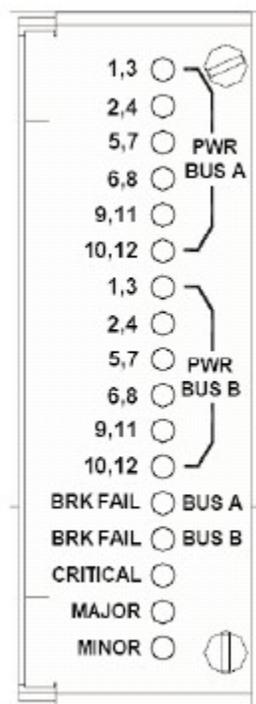
Description:

This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see [Figure 3-1](#)) identify whether the fault occurred on the input power or the output power, as follows:

- A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit.

Note: LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.

- A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.

Figure 3-1 Breaker Panel LEDs**Severity:**

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

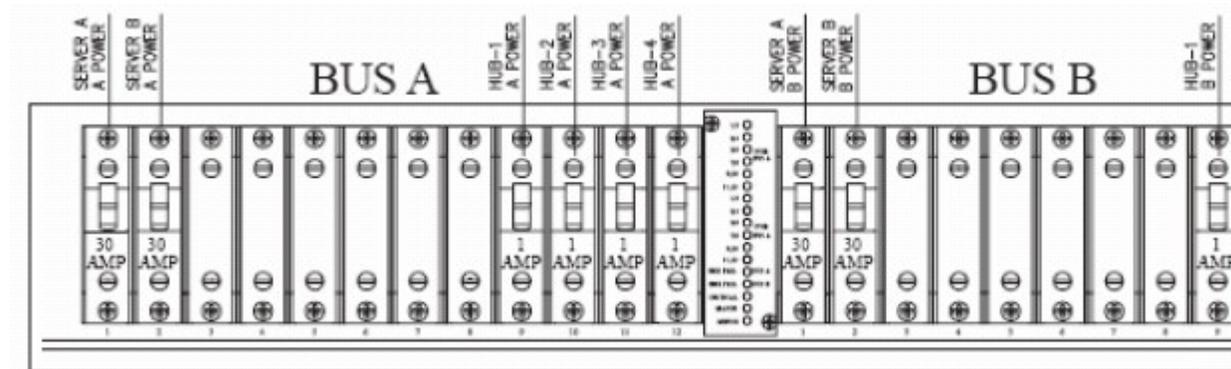
TPDBrkPnlBreakerError

Alarm ID:

TKSPLATMA26

Recovery:

1. Verify that the same alarm is displayed by both servers. The single breaker panel normally sends alarm information to both servers:
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by both servers, go to the next step.
2. For each breaker assignment, verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

Figure 3-2 Breaker Panel Setting

If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Perform the following steps to correct this problem:

- Verify that the customer provided source for the affected power feed is operational. If the power source is properly functioning, have an electrician remove the plastic cover from the rear of the breaker panel and verify the power source is indeed connected to the input power feed connector on the rear of the breaker panel. Correct any issues found.
- Check the LEDs in the PWR BUS A group and the PWR BUS B group again.
 - a. If the LEDs are now illuminated Green, the issue has been resolved. Proceed to step 4 to verify that the alarm has been cleared.
 - b. If the LEDs are still illuminated Red, continue to the next sub-step.
- Have the electrician verify the integrity of the input power feed. The input voltage should measure nominally -48VDC (that is, between -41VDC and -60VDC). If the supplied voltage is not within the acceptable range, the input power source must be repaired or replaced.

Note:

Be sure the voltmeter is connected properly. The locations of the BAT and RTN connections are in mirror image on either side of the breaker panel.

If the measured voltage is within the acceptable range, the breaker panel may be malfunctioning. The breaker panel must be replaced.

- Check the LEDs in the PWR BUS A group and the PWR BUS B group again after the necessary actions have been taken to correct any issues found
 - a. If the LEDs are now illuminated Green, the issue has been resolved and proceed to step 4 to verify that the alarm has been cleared.
 - b. If the LEDs are still illuminated Red, skip to step 5
- 3. Check the BRK FAIL LEDs for BUS A and for BUS B.
 - If one of the BRK FAIL LEDs is illuminated Red, then one or more of the respective Input Breakers has tripped. (A tripped breaker is indicated by the

toggle located in the center position.) Perform the following steps to repair this issue:

- a. For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.
 - b. After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, run syscheck and contact [My Oracle Support](#)
4. If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise it is recommended to run syscheck and contact [My Oracle Support](#)
 5. Run syscheck.
 - If the alarm has been cleared, the problem is resolved.
 - If the problem has not been resolved, it is recommended to contact [My Oracle Support](#)

32326 - Breaker panel monitoring error

Alarm Group:

PLAT

Description:

This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself.

Note: When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm:

- 32324 – Breaker panel feed error
- 32325 – Breaker panel breaker error

until the Breaker Panel Monitoring Error has been corrected.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdBrkPnlMntError

Alarm ID:

TKSPLATMA27

Recovery:

1. Verify that the same alarm is displayed by both servers (the single breaker panel normally sends alarm information to both servers):
 - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
 - If this alarm is displayed by both servers, go to the next step.
2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).
3. Run syscheck..
 - If the alarm has been cleared, the problem is resolved.
 - If the alarm has not been cleared, it is recommended to contact [My Oracle Support](#)

32327 - Server HA Keepalive error

Alarm Group:

PLAT

Description:

This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:
tpdHaKeepaliveError

Alarm ID:
TKSPLATMA28

Recovery:

1. Determine if the mate server is currently down and bring it up if possible.
2. Determine if the keepalive interface is down.
3. Determine if heartbeat is running (service TKLCha status).

Note: This step may require command line ability.

4. It is recommended to contact [My Oracle Support](#).

32328 - DRBD is unavailable

Alarm Group:
PLAT

Description:
This alarm indicates that DRBD is not functioning properly on the local server. The DRBD state (disk state, node state, and/or connection state) indicates a problem.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDrbdUnavailable

Alarm ID:
TKSPLATMA29

Recovery

1. It is recommended to contact [My Oracle Support](#).

32329 - DRBD is not replicating

Alarm Group:
PLAT

Description:

This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDrbdNotReplicating

Alarm ID:

TKSPLATMA30

Recovery

1. It is recommended to contact [My Oracle Support](#).

32330 - DRBD peer problem

Alarm Group:

PLAT

Description:

This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDrbdPeerProblem

Alarm ID:
TKSPLATMA31

Recovery

1. It is recommended to contact the [My Oracle Support](#).

32331 - HP disk problem

Alarm Group:
PLAT

Description:
This major alarm indicates that there is an issue with either a physical or logical disk in the HP disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskProblem

Alarm ID:
TKSPLATMA32

Recovery:

1. Run syscheck in verbose mode.
2. If "Cache Status" is OK and "Cache Status Details" reports a cache error was detected so diagnostics should be run, there probably is no battery and data was left over in the write cache not getting flushed to disk and won't since there is no battery.
3. If "Cache Status" is "Permanently Disabled" and "Cache Status Details" indicated the cache is disabled, if there is no battery then the firmware should be upgraded.
4. Re-run syscheck in verbose mode if firmware upgrade was necessary.
5. If the condition persists, it is recommended to contact [My Oracle Support](#) and provide the system health check output. The disk may need to be replaced.

32332 - HP Smart Array controller problem

Alarm Group:

PLAT

Description:

This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHpDiskCtrlrProblem

Alarm ID:

TKSPLATMA33

Recovery:

1. Run syscheck in verbose mode.
2. If condition persists, it is recommended to contact [My Oracle Support](#) and provide the system health check output.

32333 - HP hpacucliStatus utility problem

Alarm Group:

PLAT

Description:

This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus/hpDiskStatus daemon is either not running, or hung.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:
tpdHPACUCLIPProblem

Alarm ID:
TKSPLATMA34

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the HP disk status daemon is running. If not running verify that it was not administratively stopped.

Note: The disk status daemon is named either TKLChpacucli or TPDhpDiskStatus in more recent versions of TPD.

- a. Executing "status TPDhpDiskStatus", or "status TKLChpacucli" depending on TPD release, should produce output indicating that the process is running.
4. If not running, attempt to start the HP disk status process :
"start TPDhpDiskStatus", or if appropriate "start TKLChpacucli" .
5. Verify that there are no hpssacli, or hpacucli, error messages in /var/log/messages. If there are this could indicate that the HP utility is hung. If the HP hpssacli utility, or hpacucli utility, is hung, proceed with next step.
6. It is recommended to contact [My Oracle Support](#) and provide the system health check output, and savelogs_plat output.

32334 - Multipath device access link problem

Alarm Group:
PLAT

Description:
One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMpathDeviceProblem

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32335 - Switch link down error

Alarm Group:
PLAT

Description:
The link is down.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwitchLinkDownError

Alarm ID:
TKSPLATMA36

Recovery:

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, it is recommended to contact [My Oracle Support](#) to determine who should verify port settings on both the server and the switch.

32336 - Half Open Socket Limit

Alarm Group:
PLAT

Description:
This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity:
Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHalfOpenSockLimit

Alarm ID:

TKSPLATMA37

Recovery:

1. Run syscheck in verbose mode.
2. Determine what process and address reports a state of SYN_RECV and collect data:
 - netstat -nap.
3. It is recommended to contact [My Oracle Support](#) and provide the system health check output and collected data.

32337 - Flash Program Failure

Alarm Group:

PLAT

Description:

This alarm indicates that there was an error while trying to update the firmware flash on the E5-APP-B cards.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdFlashProgramFailure

Alarm ID:

TKSPLATMA38

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32338 - Serial Mezzanine Unseated

Alarm Group:

PLAT

Description:

This alarm indicates that a connection to the serial mezzanine board may not be properly seated.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSerialMezzUnseated

Alarm ID:

TKSPLATMA39

Recovery:

1. Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.
2. It is recommended to contact [My Oracle Support](#) if reseating the cables does not clear the alarm.

32339 - TPD Max Number Of Running Processes Error

Alarm Group:

PLAT

Description:

This alarm indicates that the maximum number of running processes has reached the major threshold.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdMaxPidLimit

Alarm ID:

TKSPLATMA40

Recovery:

1. Run syscheck in verbose mode.
2. Execute 'pstree' to see what pids are on the system and what process created them. Collect the output of command, and review the output to determine the process responsible for the alarm.
3. It is recommended to contact [My Oracle Support](#) and provide the system health check output, and pid output.

32340 - TPD NTP Daemon Not Synchronized Error

Alarm Group:

PLAT

Description:

This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdNTPDaemonNotSynchronizedError

Alarm ID:

TKSPLATMA41

Recovery:

1. Verify NTP settings and that NTP sources can be reached.

- a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
 3. If problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32341 - TPD NTP Daemon Not Synchronized Error

Alarm Group:

PLAT

Description:

This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdNTPDaemonNeverSynchronized

Alarm ID:
TKSPLATMA42

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If the ntp peer is reachable, restart the ntpd service.
3. If the problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32342 - NTP Offset Check Error

Alarm Group:
PLAT

Description:
This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:

0 (zero)

OID:

ntpOffsetCheckError

Alarm ID:

TKSPLATMA43

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If the ntp peer is reachable, restart the ntpd service.
3. If the problem persists then a reset the NTP date may resolve the issue.

Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32343 - TPD RAID disk

Alarm Group:

PLAT

Description:

This alarms indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDiskProblem

Alarm ID:

TKSPLATMA44

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32344 - TPD RAID controller problem

Alarm Group:

PLAT

Description:

This alarms indicates that RAID controller needs intervention.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDiskCtrlrProblem

Alarm ID:

TKSPLATMA45

Recovery:

1. Run syscheck in verbose mode.
2. Verify firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.

3. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32345 - Server Upgrade snapshot(s) invalid

Alarm Group:

PLAT

Description:

This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdUpgradeSnapshotInvalid

Alarm ID:

TKSPLATMA46

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. If the alarm persists, it is recommended to contact [My Oracle Support](#).

32346 - OEM hardware management service reports an error

Alarm Group:

PLAT

Description:

This alarms indicates that OEM hardware management service reports an error.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdOEMHardware

Alarm ID:

TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32347 - The hwmgmtcliStatus daemon needs intervention**Alarm Group:**

PLAT

Description:

This alarms indicates the hwmgmtcliStatus daemon is not running or is not responding.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHWMGMTCLIProblem

Alarm ID:

TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the hwmgmt process is running. If not running verify that it was not administratively stopped.
 - Running "service hwmgmt status" should produce output indicating that the process is running.

- If not running, attempt to start process "service hwmgmt status".
- 4. Determine if the TKLChwmgmtcli process is running. If not running verify that it was not administratively stopped.
 - Running "status TKLChwmgmtcli" should produce output indicating that the process is running.
 - If not running, attempt to start process "start TKLChwmgmtcli".
- 5. Verify that there are no hwmgmt error messages in /var/log/messages. If there are this could indicate that the Oracle utility is hung. If hwmgmt process is hung, proceed with next step.
- 6. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32348 - FIPS subsystem problem

Alarm Group:

PLAT

Description:

This alarm indicates the FIPS subsystem is not running or has encountered errors.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdFipsSubsystemProblem

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#) and provide the system health check output.

32349 - File Tampering

Alarm Group:

PLAT

Description:

This alarm indicates HIDS has detected file tampering.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHidsFileTampering

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32350 - Security Process Terminated

Alarm Group:

PLAT

Description:

This alarm indicates that the security process monitor is not running.

Severity:

Major

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSecurityProcessDown

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32500 - Server disk space shortage warning

Alarm Group:

PLAT

Description:

This alarm indicates that one of the following conditions has occurred:

- A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system.
- More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDiskSpaceShortageWarning

Alarm ID:

TKSPLATMI1

Recovery:

1. Run syscheck in verbose mode.
2. Examine contents of identified volume in syscheck output to determine if any large files are in the file system. Delete unnecessary files, or move files off of server. Capture output from "du -sx <file system>".
3. Capture output from "df -h" and "df -i" commands.
4. Determine processes using the file system(s) that have exceeded the threshold.
5. It is recommended to contact [My Oracle Support](#), provide the system health check output, and provide additional file system output.

32501 - Server application process error

Alarm Group:

PLAT

Description:

This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdApplicationProcessError

Alarm ID:

TKSPLATMI2

Recovery:

1. Run syscheck in verbose mode.
2. If the alarm has been cleared, then the problem is solved.
3. If the alarm has not been cleared, determine the run level of the system.
 - If system run level is not 4, determine why the system is operating at that run level.
 - If system run level is 4, determine why the required number of instances processes are not running.
4. For additional assistance, it is recommended to contact [My Oracle Support](#) and provide the syscheck output.

32502 - Server hardware configuration error

Alarm Group:

PLAT

Description:

This alarm indicates that one or more of the server's hardware components are not in compliance with specifications (refer to the appropriate hardware manual).

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHardwareConfigError

Alarm ID:

TKSPLATMI3

Recovery:

1. Run syscheck in verbose mode.
2. Contact the hardware vendor to request a hardware replacement.

32503 - Server RAM shortage warning

Alarm Group:

PLAT

Description:

This alarm is generated by the MPS syscheck software package and is not part of the TPD distribution.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdRamShortageWarning

Alarm ID:

TKSPLATMI4

Recovery

1. Refer to MPS-specific documentation for information regarding this alarm.
2. It is recommended to contact the [My Oracle Support](#).

32504 - Software Configuration Error

Alarm Group:

PLAT

Description:

This alarm is generated by the MPS syscheck software package and is not part of the PLAT distribution.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSoftwareConfigError

Recovery

1. It is recommended to contact [My Oracle Support](#).

32505 - Server swap space shortage warning

Alarm Group:

PLAT

Description:

This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

Note: For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSwapSpaceShortageWarning

Alarm ID:

TKSPLATMI6

Recovery:

1. Run syscheck in verbose mode.
2. Determine which processes are using swap.
 - a. List application processes and determine the process id.

- b. Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
 - c. Check with the router administrator to verify that the router is configured to reply to pings on that interface.
 - d. Rerun syscheck.
3. If the alarm has not cleared, it is recommended to collect the syscheck output and contact [My Oracle Support](#).

32507 - Server temperature warning

Alarm Group:

PLAT

Description:

This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdServerTemperatureWarning

Alarm ID:

TKSPLATMI8

Recovery:

1. Ensure that nothing is blocking the fan intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Run syscheck.

4. Replace the filter (refer to the appropriate hardware manual).

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the filter is replaced before the alarm cleared.

5. Run syscheck.
6. If the problem has not been resolved, it is recommended to contact [My Oracle Support](#).

32508 - Server core file detected

Alarm Group:

PLAT

Description:

This alarm indicates that an application process has failed and debug information is available.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdServerCoreFileDetected

Alarm ID:

TKSPLATMI9

Recovery:

1. It is recommended to contact [My Oracle Support](#) to create a service request.
2. On the affected server, run this command:

```
ll /var/TKLC/core
```

Add the command output to the service request. Include the date of creation found in the command output.

3. Attach core files to the [My Oracle Support](#) service request.
4. The user can remove the files to clear the alarm with this command:

```
rm -f /var/TKLC/core/<coreFileName>
```

32509 - Server NTP Daemon not synchronized

Alarm Group:

PLAT

Description:

This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdNTPDaemonNotSynchronizedWarning

Alarm ID:

TKSPLATMI10

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop

- sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32510 - CMOS battery voltage low

Alarm Group:

PLAT

Description:

The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdCMOSBatteryVoltageLow

Alarm ID:

TKSPLATMI11

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32511 - Server disk self test warning

Alarm Group:

PLAT

Description:

A non-fatal disk issue (such as a sector cannot be read) exists.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdSmartTestWarn

Alarm ID:

TKSPLATMI12

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#).

32512 - Device warning**Alarm Group:**

PLAT

Description:

This alarm indicates that either we are unable to perform an `snmpget` command on the configured SNMP OID or the value returned failed the specified comparison operation.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDeviceWarn

Alarm ID:

TKSPLATMI13

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#).

32513 - Device interface warning

Alarm Group:

PLAT

Description:

This alarm can be generated by either an SNMP trap or an IP bond error.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDeviceIfWarn

Alarm ID:

TKSPLATMI14

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#).

32514 - Server reboot watchdog initiated

Alarm Group:

PLAT

Description:

This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdWatchdogReboot

Alarm ID:
TKSPLATMI15

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32515 - Server HA failover inhibited

Alarm Group:
PLAT

Description:
This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaInhibited

Alarm ID:
TKSPLATMI16

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32516 - Server HA Active to Standby transition

Alarm Group:
PLAT

Description:
This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHaActiveToStandbyTrans

Alarm ID:

TKSPLATMI17

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32517 - Server HA Standby to Active transition

Alarm Group:

PLAT

Description:

This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHaStandbyToActiveTrans

Alarm ID:

TKSPLATMI18

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32518 - Platform Health Check failure

Alarm Group:

PLAT

Description:

This alarm is used to indicate a configuration error.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHealthCheckFailed

Alarm ID:

TKSPLATMI19

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32519 - NTP Offset Check failure

Alarm Group:

PLAT

Description:

This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the NTP server and the offset limit that the application has set for the system.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

ntpOffsetCheckWarning

Alarm ID:

TKSPLATMI20

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32520 - NTP Stratum Check failure

Alarm Group:

PLAT

Description:

This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:
ntpStratumCheckFailed

Alarm ID:
TKSPLATMI21

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32521 - SAS Presence Sensor Missing

Alarm Group:
PLAT

Description:
This alarm indicates that the T1200 server drive sensor is not working.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:

0 (zero)

OID:

sasPresenceSensorMissing

Alarm ID:

TKSPLATMI22

Recovery:

1. It is recommended to contact [My Oracle Support](#) to get a replacement sensor.

32522 - SAS Drive Missing

Alarm Group:

PLAT

Description:

This alarm indicates that the number of drives configured for this server is not being detected.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

sasDriveMissing

Alarm ID:

TKSPLATMI23

1. It is recommended to contact [My Oracle Support](#).

32523 - DRBD failover busy

Alarm Group:

PLAT

Description:

This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDrbdFailoverBusy

Alarm ID:

TKSPLATMI24

Recovery

1. A DRBD sync should not take more than 15 minutes to complete. Please wait for approximately 20 minutes, and then check if the DRBD sync has completed. If the alarm persists longer than this time period, it is recommended to contact [My Oracle Support](#).

32524 - HP disk resync

Alarm Group:

PLAT

Description:

This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHpDiskResync

Alarm ID:

TKSPLATMI25

Recovery:

1. Run syscheck in verbose mode.
2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck.
3. If the alarm persists, it is recommended to contact [My Oracle Support](#) and provide the syscheck output.

32525 - Telco Fan Warning

Alarm Group:

PLAT

Description:

This alarm indicates that the Telco switch has detected an issue with an internal fan.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdTelcoFanWarning

Alarm ID:

TKSPLATMI26

Recovery:

1. Contact the vendor to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.

Note: [My Oracle Support](#) personnel can perform an `snmpget` command or log into the switch to get detailed fan status information.

32526 - Telco Temperature Warning

Alarm Group:

PLAT

Description:

This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdTelcoTemperatureWarning

Alarm ID:

TKSPLATMI27

Recovery:

1. Lower the ambient air temperature around the switch as low as possible.
2. If the problem persists, it is recommended to contact [My Oracle Support](#).

32527 - Telco Power Supply Warning

Alarm Group:

PLAT

Description:

This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdTelcoPowerSupplyWarning

Alarm ID:

TKSPLATMI28

Recovery:

1. Verify the breaker was not tripped.
2. If the breaker is still good and problem persists, it is recommended to contact [My Oracle Support](#) who can perform a `snmpget` command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 - Invalid BIOS value

Alarm Group:

PLAT

Description:

This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdInvalidBiosValue

Alarm ID:

TKSPLATMI29

Recovery:

1. Change the BIOS values to the expected values which involves re-booting the server. It is recommended to contact [My Oracle Support](#) for directions on changing the BIOS.

32529 - Server Kernel Dump File Detected

Alarm Group:

PLAT

Description:

This alarm indicates that the kernel has crashed and debug information is available.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdServerKernelDumpFileDetected

Alarm ID:

TKSPLATMI30

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#).

32530 - TPD Upgrade Failed**Alarm Group:**

PLAT

Description:

This alarm indicates that a TPD upgrade has failed.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

TpdServerUpgradeFailed

Alarm ID:

TKSPLATMI31

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32531 - Half Open Socket Warning Limit**Alarm Group:**

PLAT

Description

This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdHalfOpenSocketWarning

Alarm ID:

TKSPLATMI32

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#).

32532 - Server Upgrade Pending Accept/Reject

Alarm Group:

PLAT

Description:

This alarm indicates that an upgrade occurred but has not been accepted or rejected yet.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdServerUpgradePendingAccept

Alarm ID:
TKSPLATMI33

Recovery:

1. Follow the steps in the application procedure to accept or reject the upgrade.

32533 - TPD Max Number Of Running Processes Warning

Alarm Group:
PLAT

Description:
This alarm indicates that the maximum number of running processes has reached the minor threshold.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMaxPidWarning

Alarm ID:
TKSPLATMI34

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact [My Oracle Support](#).

32534 - TPD NTP Source Is Bad Warning

Alarm Group:
PLAT

Description:
This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.

Severity:
Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdNTPSourceIsBad

Alarm ID:

TKSPLATMI35

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
 - a. Ensure ntpd service is running.
 - b. Verify the content of the /etc/ntp.conf file is correct for the server.
 - c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
 - d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

- a. To reset date:
 - sudo service ntpd stop
 - sudo ntpdate <ntp server ip>
 - sudo service ntpd start
4. If the problem persists, it is recommended to contact [My Oracle Support](#).

32535 - TPD RAID disk resync

Alarm Group:

PLAT

Description:

This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdDiskResync

Alarm ID:

TKSPLATMI36

Recovery:

1. Run syscheck in verbose mode.
2. If this alarm persists for several hours (depending on a load of a server, rebuilding an array can take multiple hours to finish), it is recommended to contact [My Oracle Support](#).

32536 - TPD Server Upgrade snapshot(s) warning

Alarm Group:

PLAT

Description:

This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdUpgradeSnapshotWarning

Alarm ID:

TKSPLATMI37

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. It is recommended to contact [My Oracle Support](#)

32537 - FIPS subsystem warning event

Alarm Type:

PLAT

Description:

This alarm indicates that the FIPS subsystem requires a reboot in order to complete configuration.

Severity:

Minor

Instance:

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdFipsSubsystemWarning

Recovery

1. If alarm does not clear on its own, it is recommended to contact [My Oracle Support](#).

32538 - Platform Data Collection Error

Alarm Group

PLAT

Description

Platform Data Collection Error

Severity

Minor

Instance

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score

Normal

Auto Clear Seconds

0 (zero)

OID

tpdPdcError

Recovery

1. Run `/usr/TKLC/plat/bin/pdcAdm`. If ran as admusr, use sudo to run the command.
2. If this command fails, it is recommended to collect the output and contact [My Oracle Support](#).

32539 - Server Patch Pending Accept/Reject

Alarm Group

PLAT

Description

Server Patch Pending Accept/Reject

Severity

Minor

Instance

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score

Normal

Auto Clear Seconds

0 (zero)

OID

tpdServerPatchPendingAccept

Recovery

1. Accept or reject the patch per the application documentation procedure.

32540 - CPU Power limit mismatch

Alarm Group:

PLAT

Description:

The BIOS setting for CPU Power Limit is different than expected.

Severity:

Minor

Instance:

N/A

HA Score:

Normal

Auto Clear Seconds:

0 (zero)

OID:

tpdCpuPowerLimitMismatch

Alarm ID:

TKSPLATMI41

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32700 - Telco Switch Notification

Alarm Group:

PLAT

Description

Telco Switch Notification

Severity

Info

Instance

May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score

Normal

Auto Clear Seconds

86400

OID

tpdTelcoSwitchNotification

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32701 - HIDS Initialized

Alarm Group:

PLAT

Description:

This alarm indicates HIDS was initialized.

Default Severity:

Info

OID:

tpdHidsBaselineCreated

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32702 - HIDS Baseline Deleted**Alarm Group:**

PLAT

Description:

HIDS baseline was deleted.

Default Severity:

Info

OID:

tpdHidsBaselineDeleted

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32703 - HIDS Enabled**Alarm Group:**

PLAT

Description:

HIDS was enabled.

Default Severity:

Info

OID:

tpdHidsEnabled

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32704 - HIDS Disabled

Alarm Group:

PLAT

Description:

HIDS was disabled.

Default Severity:

Info

OID:

tpdHidsDisabled

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32705 - HIDS Monitoring Suspended

Alarm Group:

PLAT

Description:

HIDS monitoring suspended.

Default Severity:

Info

OID:

tpdHidsSuspended

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32706 - HIDS Monitoring Resumed

Alarm Group:

PLAT

Description:

HIDS monitoring resumed.

Default Severity:

Info

OID:

tpdHidsResumed

Recovery:

1. It is recommended to contact [My Oracle Support](#).

32707 - HIDS Baseline Updated

Alarm Group:

PLAT

Description:

HIDS baseline updated.

Default Severity:

Info

OID:

tpdHidsBaselineUpdated

Recovery:

1. It is recommended to contact [My Oracle Support](#).

QP (70000-70999)

The **QBus Platform (QP)** software provides an execution environment for Java-based applications, which are the **Multiprotocol Routing Agent (MRA)** devices, **Multimedia Policy Engine (MPE)** devices, or the **Configuration Management Platform (CMP)** server. QP provides common interfaces into databases, event logging, SNMP, and cluster state. Two servers in the cluster provide 1+1 High-Availability (HA) protection. The application executes on one server. The other server acts as a hot standby in case the first server fails to provide service.

70001 – QP_procMgr failed

Alarm Type

QP

DescriptionThe QP-`procMgr` process has failed. This process manages all PCRf software.**Default Severity**

Critical

Instance

N/A

HA Score

Failed

Clearing ActionThis alarm is cleared by `qp-procMgr` after `qp-procMgr` is restarted.**OID**

QPProcMgrFailed

Recovery:

1. If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact [My Oracle Support](#).

70002 – QP Critical process failed

Alarm Type

QP

Description

The QP_procmgr has detected that one of the critical processes it monitors has failed.

Default Severity

Critical

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically.

OID

QPCriticalProcFailed

Recovery:

1. This alarm automatically clears as Policy processes are restarted.
2. If the alarm does not clear automatically within a few seconds, or if the alarm occurs frequently, contact [My Oracle Support](#).

70003 – QP Non-critical process failed

Alarm Type

QP

Description

The QP_procmgr has detected that one of the non-critical processes it monitors has failed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 seconds.

OID

QPNonCriticalProcFailed

Recovery:

1. If the alarm occurs infrequently, monitor the health of the system.
2. If the alarm occurs frequently, contact [My Oracle Support](#).

70004 – QP Processes down for maintenance

Alarm Type

QP

Description

The QP processes have been brought down for maintenance.

Default Severity

Major

Instance

N/A

HA Score

Failed

Clearing Action

This alarm clears when the QP processes are restarted and exit maintenance.

OID

QPMaintShutdown

Recovery:

1. If the alarm is occurring, confirm that the server is down for maintenance.

70007 - QP Resource Not Ready

Alarm Type: QP

Description: Not all QP resources are ready.

Severity: Critical

Instance: N/A

HA Score: Failed

Clearing Action: To clear the alarm, one of the following conditions must be met:

- All route resources managed by QP are functional.
- The alarm auto clears after 300 sec.

OID: QPResourceNotReady

Recovery:

Note: Static routes will be reapplied during the promotion of a node to Active. If a failure occurs while reapplying static routes, promoting a node to Active in turn will fail.

Note: Currently, only the route resource is managed by QP.

Note: The main log location for troubleshooting route resource not ready issues is here: `/var/camiant/log/qpRouteTool.log`. Trace logs for `qp_procmgr` and `routemgr` may be needed for troubleshooting. Trace logs can be captured using commands: `tr.cat qp_procmgr > /qp_procmgr.trace` `tr.cat routemgr > /routemgr.trace`

1. If the original Active node can go back to Active, the current node will be demoted after failure. In this situation, no workaround is needed because the system will recover automatically. However, you need to check the reason that applying routes fails so that it does not occur in the next failover.
2. If the original Active node can not go back to Active, the current node will repeatedly attempt to go Active. It will not become Active until the application of static routes is successful. In this situation, the reason for the failure needs to be checked case by case so that the system can be recovered.

70010 – QP Failed Server-backup Remote Archive Rsync

Alarm Type

QP

Description

A scheduled backup failed to synchronize the local server-backup archive with the remote server-backup archive.

- Hostname=<hostname | IPaddr>
- path=<path>
- errorcode=<rsync error>

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 64800 seconds (18 hours).

OID

QPServerBackupRsyncFailed

Recovery:

1. Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

70011 – QP Failed System-backup Remote Archive Rsync

Alarm Type

QP

Description

A scheduled backup failed to synchronize the local system-backup archive with the remote system-backup archive.

Hostname=<host name | IP addr>, user=<user>, path=<path>,errorcode=<rsync error>

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 64800 seconds (18 hours).

OID

QPSystemBackupRsyncFailed

Recovery:

1. Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

70012 – QP Failed To Create Server Backup

Alarm Type

QP

Description

A scheduled backup failed to create the local server-backup file.

Failure-reason=<errorcode>

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 64800 seconds (18 hours).

OID

QPServerBackupFailed

Recovery:

1. Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

70013 – QP Failed To Create System Backup**Alarm Type**

QP

Description

A scheduled backup failed to create the local system-backup file.
Failure-reason=<errorcode>

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 64800 seconds (18 hours).

OID

QPSystemBackupFailed

Recovery:

1. Check that the parameters are correct; take corrective action based on the returned error code details for alarms 70010 and 70011. Then re-attempt server-backup remote archive synchronization.

70015 – Route Add Failed**Alarm Type**

QP

Description

VIP Route Add Failed — VIP route add failed to re-apply during VIP event.
The alarm displays the following information:

- IP-Type
- Route-Type
- Network

- Destination
- Gateway-Address
- Error Message

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 3600 seconds (60 minutes).

OID

QpAddRouteFailed

Recovery:

1. Use Platcfg Routing menu to repair the route manually.

70016 – No Available VIP Route

Alarm Type

QP

Description

This alarm is raised when the application of a route item with VIP as the preferred source fails because the VIP is not configured.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

When VIP becomes available, this alarm is cleared. If the route item is deleted, this alarm is also cleared.

OID

QPNoVipForRoute

Recovery:

1. Check route configuration.
2. If route is configured correctly, this alarm can be ignored.

70017 – No Available Static IP

Alarm Type

QP

Description

This alarm is raised when the application of a route item with STATIC IP as preferred source fails because the STATIC IP is not available.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

When a STATIC IP becomes available, this alarm is cleared. If the route item is deleted, this alarm is also cleared.

OID

QPNoStaticIPForRoute

Recovery:

1. Check the route configuration and check the STATIC IP status.
2. Check route configuration; if route is configured correctly, this alarm can be ignored.

70020 – QP Master database is outdated

Alarm Type

QP

Description

The current MYSQL master server has an outdated database.

Default Severity

Critical

Instance

N/A

HA Score

Degraded

Clearing Action

This alarm clears when the master server either is made a slave server or if a database restore action clears the condition.

OID

QPMysqlMasterOutdated

Recovery:

1. Once the condition has occurred, the 80003 event will be sent once a minute. Wait until all of the expected servers are being reported. It is important to wait because the best slave might be undergoing a restart and its DB Level will not be known until after the restart completes.
2. Use the information in 80003 to select the new master candidate.
3. Except for the current master and the master candidate, put all of the other servers into forced standby.
4. If the best secondary server is in the same cluster (the most common case), perform a failover by restarting the current active blade. If the best secondary server is in a separate cluster, then a site promotion is necessary.
5. Remove the forced standby settings on the other slaves.
6. If none of the slaves are good candidates, perform a database restore.
 - a. Put all of the slave servers into forced standby state.
 - b. Perform a restore on the active server.

The restore will clear the condition.
 - c. Take the slave servers out of the standby state.

70021 – QP slave database is unconnected to the master**Alarm Type**

QP

Description

The MySQL slave is not connected to the master.

Default Severity

Major

Instance

N/A

HA Score

Failed

Clearing Action

This alarm clears automatically when the slave server connects to the master server.

OID

QPMysqlSlaveUnconnected

Recovery:

1. No action required unless the alarm does not clear within a few hours.

2. If the problem persists, contact [My Oracle Support](#).

70022 – QP Slave database failed to synchronize

Alarm Type

QP

Description

The MySQL slave failed to synchronize with the master.

Default Severity

Major

Instance

N/A

HA Score

Failed

Clearing Action

This alarm clears when the slave server synchronizes with the master server.

OID

QPMySQLSlaveSyncFailure

Recovery:

1. No action required unless the alarm does not clear within a few hours.
2. If the problem persists, contact [My Oracle Support](#).

70023 – QP Slave database lagging the master

Alarm Type

QP

Description

The MySQL slave is lagging the master —The MySQL slave server is connected to the master server but its database has fallen behind the master database.

Default Severity

Minor

Instance

N/A

HA Score

Degraded

Clearing Action

This alarm clears automatically when the slave database is synchronized with the master database.

OID

QPMySQLSlaveLagging

Recovery:

1. No action required unless the alarm does not clear within a few hours or the condition is repeatedly set and cleared.
2. If either of the problems persists, contact [My Oracle Support](#).

70024 - QP Slave database is prevented from synchronizing with the master

Alarm Type

QP

Description

The MySQL slave has been prevented from synchronizing with the master—The MySQL slave database has been prevented from synchronization with the master database because the master database is outdated.

Default Severity

Critical

Instance

N/A

HA Score

Degraded

Clearing Action

This alarm clears when the slave database is synchronized with the master database. This alarm is set on the slave server and will only occur when the active server on the primary site has set alarm 70020. This alarm clears automatically when the slave database is synchronized with the master database.

OID

QPMySQLSlaveSyncPrevented

Recovery:

1. Diagnose the CMP master server to clear its 70020 alarm.
2. Once alarm 70020 is cleared, the slave server will clear alarm 70024.

70025 – QP Slave database is a different version than the master

Alarm Type

QP

Description

The MySQL slave has a different schema version than the master.

This alarm is set by the CMP Slave Server during a CMP Server Upgrade or Backout, when the CMP Master Server DB is a different version than the CMP Slave Server DB.

Default Severity

Critical

Instance

N/A

HA Score

Normal

Clearing Action

The slave server clears the alarm when the master DB version is equal to the slave DB version.

OID

QPMySQLSchemaVersionMismatch

Recovery:

1. The Slave Server clears the alarm when the Master Server and the Slave Server again have the same version.

70026 – QP Server Symantec NetBackup Operation in Progress

Alarm Type

QP

Description

Server is performing a Symantec NetBackup Operation.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Alarm clears when the NetBackup client operation has completed.

OID

QPNetBackupInProgress

Recovery:

1. When operation is complete, alarm should clear.
2. If the alarm does not clear within a few hours, then check the NetBackup Server logs.
3. If the NetBackup Server logs have no errors or if the alarm is occurring over and over, contact [My Oracle Support](#).

70027 – QP Server Network Config Error

Alarm Type

QP

Description

QP Server Network Error.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Autoclears in 1800 seconds (30 minutes).

OID

QPServerNetworkConfigError

Recovery

1. Correct the indicated networking configuration.
2. If the problem persists, contact [My Oracle Support](#).

70028 – QP bonded interface is down

Alarm Type

QP

Description

OAM bonded interface bond0 is down; Signaling bonded interface bond1 is down; Signaling bonded interface bond2 is down.

Default Severity

Critical

Instance

OAM, SIGA, SIGB

HA Score

Degraded

Clearing Action

Process `qp_hamonitor` has detected the VIP is not defined on this bonded network interface; VIP is defined on this bonded network interface and `qp_hamonitor` process has detected the interface is up.

OID

QPBondedInterfaceDown

Recovery:

1. Reset the OAM network interface and run process `qp_hamonitor` to clear the alarm.
2. If the `qp_hamonitor` process does not clear the alarm, or if the alarm does not clear automatically, or if the alarm is persists, contact [My Oracle Support](#)

70029 – QP peer node bonded interface is down

Alarm Type

QP

DescriptionQP Peer Node $\{host\ name\}$ ($\{ip\ addr\}$) bonded interface bond0 (OAM) is down.**Default Severity**

Critical

Instance

Peer_OAM

HA Score

Normal

Clearing Action

Process `qp_hamonitor` will clear the alarm once the OAM network interface is up. The alarm will also clear automatically after 60 seconds.

OID

QPPeerBondedInterfaceDown

Recovery:

1. Reset the OAM network interface and run process `qp_hamonitor` to clear the alarm.
2. If the `qp_hamonitor` process does not clear the alarm, or if the alarm does not clear automatically, or if the alarm is persists, contact [My Oracle Support](#)

70030 – QP backplane bonded interface is down

Alarm Type

QP

Description

Backplane bonded interface is down.

Default Severity

Critical

Instance

Backplane_bond3

HA Score

Normal

Clearing Action

Process `qp_hamonitor` has detected the bonded backplane network interface has been restored or the alarm has been raised for 60 seconds.

OID
QPBackplaneBondedInterfaceDown

Recovery:

1. Restore the bonded backplane network interface that is down and the `qp_hamonitor` process will clear the alarm.

70031 – QP degrade because one or more interfaces are down

Alarm Type
QP

Description
HA status is degraded because selected interface(s) (*\$/OAM, SIGA, or SIGB*) are down.

Default Severity
Critical

Instance
OAM or SIGA or SIGB

HA Score
Failed

Clearing Action
Alarm clears when process `qp_hamonitor` has detected all OAM, SIGA and SIGB network interfaces are up. Alarm also clears automatically after 60 seconds.

OID
QPInterfacesDegrade

Recovery:

1. Reset the interfaces that are down and run the `qp_hamonitor` process to clear the alarm.
2. If this does not clear the alarm, or if the alarm does not automatically clear, or if the alarm persists, contact [My Oracle Support](#).

70032 – QP direct link does not work as configuration

Alarm Type
QP

Description
QP degrade because one or more interfaces are down.
This alarm is due to the incorrect configuration of backplane so that it cannot be applied to the system.

Default Severity
Notice

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

QPBpMismatch

Recovery:

1. Check the validity of backplane IP Address and Comcol table LogicPath.

70038 – QP has blocked IPv4 traffic on an OAM interface**Alarm Type**

QP

Description

This alarm is raised on each server if IPv4 is blocked on an OAM. After `qpIPv4Harvest --block_oam_ipv4` is finished successfully, this alarm is raised.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm is cleared by `qpIPv4Harvest -harvest_oam_only` or `qpIPv4Harvest -harvest_oam_all`.

OID

QPHasBlockedIPv4

Recovery:

1. Rollback changes in `qpIPv4Harvest -block_oam_ipv4`; Or continue to run `qpIPv4Harvest -harvest_oam_only`.

70039 – QP has blocked IPv4 traffic on all interfaces**Alarm Type**

QP

Description

This alarm is raised on each server if IPv4 is blocked on all interfaces. After `qpIPv4Harvest -block_all_ipv4` is finished successfully, this alarm is raised.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm is cleared by `qpIPv4Harvest -harvest_all`.

OID

QPHasBlockedIPv4

Recovery:

1. Rollback changes in `qpIPv4Harvest -block_all_ipv4`; Or continue to run `qpIPv4Harvest -harvest_all`.

70040 – Failure to block IPv4 on the OAM interface**Alarm Type**

QP

Description

This alarm is raised when there is a failure to block IPv4 on an OAM interface.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm will be cleared automatically in 60 minutes. Or it can be cleared once the cluster/site has successfully blocked IPv4 on an OAM interface.

OID

QPFailedToBlockOAMIPv4

Recovery:

1. Correct the error conditions and run `qpIPv4Harvest -block_oam_ipv4` again.

70041 – Failure to block IPv4 on the all interfaces**Alarm Type**

QP

Description

This alarm is raised when there is a failure to block IPv4 on all interfaces.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm will be cleared automatically in 1 hour. Or it can be cleared once the cluster/site has successfully blocked IPv4 on all interfaces.

OID

QPFailedToBlockAllIpv4

Recovery:

1. Correct the error conditions, and run `qpIPv4Harvest -block_all_ipv4` again.

70042 – Failure to remove OAM IPv4 addresses from the cluster/site**Alarm Type**

QP

Description

This alarm is raised when there is a failure to remove OAM IPv4 addresses from cluster/site

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm will be cleared automatically in 1 hour. Or it can be cleared once the OAM IPv4 addresses are successfully removed.

OID

QPFailedToRemoveOAMIpv4

Recovery:

1. Correct the error conditions and do the harvest again.

70043 – Failure to remove all IPv4 addresses from the cluster/site**Alarm Type**

QP

Description

This alarm is raised when there is a failure to remove all IPv4 addresses from cluster/site.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm will be cleared automatically in 1 hour. Or it can be cleared once all IPv4 addresses are successfully removed.

OID

QPFailedToRemoveAllIpv4

Recovery:

1. Correct the error conditions and do harvest again.

70044 – Failure to rollback changes for removing IPv4 addresses

Alarm Type

QP

Description

This alarm is raised when there is a failure to rollback changes for removing IPv4 addresses.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm will be cleared automatically in 1 hour. Or it can be cleared once the rollback action finished successfully.

OID

QPFailedToRollbackRecaptureIpv4

Recovery:

1. Correct the error conditions and do the rollback again.

70045 – DNS Server is not available

Alarm Type

QP

Description

If DNS servers are configured on PCRF nodes, those nodes will use DNS servers. Process `qp_monitor` will check DNS availability at the runtime of every node. If a DNS server is found unavailable, QP alarm 70045 is triggered.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm will be cleared automatically after 120 seconds.

OID

QPDNSServerIsNotAvailable

Recovery:

1. If the alarm message is **No reply from server**, the server could not be reached or the connection has timed out. To resolve:
 - a. Check the route and firewall settings from the PCRF node reporting the alarm to determine if a DNS server can be accessed.
 - b. Repair the access to the specific DNS server.
2. If the alarm message is **Internal error** the DNS server IP address format is incorrect. To resolve:
 - a. Use Platcfg commands `Policy Configuration -> Perform Initial Configuration` to check the IP address format of the DNS server:

70050 – QP Timezone change detected**Alarm Type**

QP

Description

Time zone has been changed using `platcfg` commands `Server Configuration -> Time Zone -> Edit`. The application needs to be restarted after this change.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears when the application is restarted (qp_procmgr restarted). This is not an auto-clear alarm.

OID

QPTimezonechangedetected

Recovery:

1. Log in to the server with root privileges.
2. Execute the command `service qp_procmgr restart`.
3. If the alarm persists, collect savelogs and contact [My Oracle Support](#).

70500 – System Mixed Version

Alarm Type

QP

Description

There are multiple software versions running in the system because of an upgrade or backout. This alarm is raised when the upgrade director determines that different versions of code are running in the topology. This is expected during an upgrade. It is intended to be a signal that further upgrade activity is required before the system is fully consistent.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

SystemMixedVersion

Recovery:

1. The upgrade director will clear this condition once all servers are running a consistent version.
2. If the alarm does not clear automatically, contact [My Oracle Support](#).

70501 – Cluster Mixed Version

Alarm Type

QP

Description

There are multiple software versions running in a cluster because of an upgrade or backout. Since the cluster is in mixed version, its behavior is likely to be impaired (for example, loss of redundancy/replication). Certain operations may not be possible for the cluster while this alarm is asserted. This alarm is raised when the upgrade director determines that different versions of code are running in the specified cluster. This is expected during an upgrade. It is intended to be a signal that further upgrade activity is required before the cluster is fully consistent.

Default Severity

Minor

Instance

The Comcol ID of the cluster.

HA Score

Normal

Clearing Action

N/A

OID

ClusterMixedVersion

Recovery:

1. The upgrade director will clear this condition once all servers in the cluster are running a consistent version.
2. If the alarm does not clear automatically, contact [My Oracle Support](#).

70502 – Cluster Replication Inhibited

Alarm Type

QP

Description

The upgrade director will inhibit replication to a server if it determines that replication would result in a corrupted database. This can happen if there is an incompatibility between different versions.

Default Severity

Minor

Instance

The Comcol ID of the server.

Note: The alarm text will contain the proper host name of the server.

HA Score

Normal

Clearing Action

N/A

OID
ClusterReplicationInhibited

Recovery:

1. Once the server completes the upgrade or backout, the upgrade director will clear the inhibition and the alarm.
2. If the alarm does not clear automatically, contact [My Oracle Support](#).

70503 – Server Forced Standby

Alarm Type
QP

Description
The upgrade director will place a server into forced standby if it is NOT running the same version of software as the active server in the cluster. This alarm signals that the upgrade director has taken this action.

Default Severity
Minor

Instance
The Comcol ID of the server.

Note: The alarm text will contain the proper hostname of the server.

HA Score
Normal

Clearing Action
N/A

OID
ServerForcedStandby

Recovery:

1. When the server completes the upgrade or backout, the upgrade director will take the server out of forced standby.
2. If the alarm does not clear automatically, contact [My Oracle Support](#).

70505 – ISO Mismatch

Alarm Type
QP

Description
The server's ISO is not the expected version. This alarm is raised when the upgrade director determines that the 'pending ISO' (the one that would be installed if we attempted an upgrade) is not consistent with what is expected (for example, the wrong version).

Default Severity

Minor

Instance

The Comcol ID of the server.

Note: The alarm text will contain the proper host name of the server.

HA Score

Normal

Clearing Action

N/A

OID

ISOMismatch

Recovery:

1. Have the operator remove the offending ISO from `/var/TKLC/log` on the affected machine.
2. If the alarm does not clear automatically, contact [My Oracle Support](#).

70506 – Upgrade Operation Failed

Alarm Type

QP

Description

An action initiated by the upgrade director has failed. Click **Alarm Details** associated with the alarm in the CMP GUI to find the root cause of the failed upgrade action.

Default Severity

Minor

Instance

The Comcol ID of the server.

Note: The alarm text will contain the proper host name of the server.

HA Score

Normal

Clearing Action

N/A

OID

UpgradeOperationFailed

Recovery:

1. Make changes as detailed in the **Alarm Detail** associated with the alarm and then re-attempt the failed upgrade action.
2. If the issues cannot be resolved, collect savelogs and contact [My Oracle Support](#).

70507 – Upgrade In Progress

Alarm Type

QP

Description

An upgrade or backout action on a server is in progress.

Default Severity

Minor

Instance

The Comcol ID of the server.

Note: The alarm text will contain the proper host name of the server.

HA Score

Normal

Clearing Action

N/A

OID

UpgradeInProgress

Recovery:

1. Once the upgrade/backout process has completed, the upgrade director will clear this alarm.
2. If the alarm does not clear automatically, contact [My Oracle Support](#).

70508 – Server Is Zombie

Alarm Type

QP

Description

A server has failed an upgrade or backout and now is in an unknown state.

Default Severity

Critical

Instance

The Comcol ID of the server.

Note: The alarm text will contain the proper host name of the server.

HA Score

Normal

Clearing Action

N/A

OID

ServerIsZombie

Recovery:

1. If alarm 70506 is also triggered, make changes as detailed in the **Alarm Detail** associated with alarm 70506 and then re-attempt the failed upgrade action to resolve both alarms.
2. If the alarm persists, collect savelogs and contact [My Oracle Support](#).

Policy Server Alarms (71000-79999)

This section provides a list of Policy Server alarms (71000-79999) which are generated by policy devices, such as MPE devices and MRA devices.

71001 – Remote Diversion Not Possible

Alarm Type

PCRF

Description

This alarm occurs when all other associated MRA devices are currently unavailable for remote diversion.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Auto clear after 7200 seconds.

OID

RemoteDiversionNotPossible

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

71002 – OM Stats Parse Error

Alarm Type

PCRF

Description

OM statistics task could not parse statistics information.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Auto clears after 7200 seconds or when OM statistics are run again.

OID

OmStatsParseError

Recovery:

1. Check to ensure Policy server version is the same as the CMP version. If the versions are different, upgrade the server version to be the same as the CMP version.

71003 – OM Stats Exception Error**Alarm Type**

PCRF

Description

OM statistics task could not generate particular statistics due to an exception.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Auto clear after 7200 seconds (120 minutes) or when OM statistics are run again.

OID

OmStatsExceptionError

Recovery:

1. Check to ensure Policy server version is the same as the CMP version. If the versions are different, upgrade the server version to be the same as the CMP version.

2. Check MySQL status to ensure there is not an exception in the DC log.

71004 – AM Conn Lost

Alarm Type

PCRF

Description

AM socket closed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

AM connection restored to remote peer.

OID

AMConnLost

Recovery:

1. Check the availability of the AM.
2. Check the AM log for a recent failover or other operations that can interrupt communications.
3. If the AM has not failed, make sure that the path from the AM to the MPE device (port 3918) is operational.
4. If the problem persists, contact [My Oracle Support](#).

71005 – OM Stats Value Exceed Error

Alarm Type

PCRF

Description

OM statistics value has been truncated to fit the data size.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Auto clears after 7200 seconds or when OM statistics are run again.

OID

OmStatsValueExceedError

Recovery:

1. Check whether the list of IP addresses in a Network Element Diameter SCTP connection association value exceeds 255 in length. If found, correct the value length.

71101 – DQoS Downstream Connection Closed**Alarm Type**

PCRF

Description

DQoS Downstream connection is closed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

DQoS connection restored to a remote peer.

OID

DqosDownstreamConnectionClosed

Recovery:

1. Check configuration and availability of the downstream element.
2. Check the downstream element for a reboot or other service interruption.
3. .If the downstream element has not failed, make sure that the network path from the MPE device to the downstream element is operational.
4. If the problem persists, contact [My Oracle Support](#).

71102 – MSC Conn Lost**Alarm Type**

PCRF

Description

MSC connection lost. The connection was lost to the specified CMTS or downstream policy server.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to a remote peer is restored.

OID

MSCConnLost

Recovery:

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (port 3918) is operational.
4. If the problem persists, contact [My Oracle Support](#).

71103 – PCMM Conn Lost

Alarm Type

PCRF

Description

PCMM connection lost. The connection was lost to the specified CMTS or downstream policy server.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Alarm clears when the connection to a remote peer is restored. The alarm also clears automatically after 7200 seconds.

OID

PCMMConnLost

Recovery:

1. Check configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.

3. If the element has not failed, make sure that the network path from the MPE device to the element (port 3918) is operational.
4. If the problem persists, contact [My Oracle Support](#).

71104 – DQOS AM Connection Closed

Alarm Type

PCRF

Description

DQoS AM Connection Closed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to a remote peer is restored.

OID

DqosAmConnectionClosed

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

71204 – SPC Conn Closed

Alarm Type

PCRF

Description

SPC connection closed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to a remote peer is restored.

OID

SPCConnClosed

Recovery:

1. Check configuration and availability of the SPC element. Check the MPE device for a reboot or other service interruption.
2. If the MPE device has not failed, make sure that the network path from the MPE device to the SPC device is operational.
3. If the problem persists, contact [My Oracle Support](#).

71402 – Connectivity Lost

Alarm Type

PCRF

Description

Diameter connection socket is closed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 7200 seconds or the connection to a Diameter peer is restored.

OID

ConnectivityLost

Recovery:

1. Check the configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the network element has not failed, ensure the network path from the device to the network element is operational.
4. If the problem persists, contact [My Oracle Support](#).

71403 – Connectivity Degraded

Alarm Type

PCRF

Description

A connection with a Diameter peer has been closed by a network element.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 7200 seconds or the connection to a Diameter peer is restored.

OID

ConnectivityDegraded

Recovery:

1. Check the configuration and availability of the network element.
2. Check the network element for a reboot or other service interruption.
3. If the network element has not failed, ensure the network path from the device to the network element is operational.
4. If the problem persists, contact [My Oracle Support](#).

71408 – Diameter New Conn Rejected

Alarm Type

PCRF

Description

Diameter new connection rejected as an already functioning one exists. A Diameter peer (identified by its Diameter Identity) attempted to establish a connection with the device although it already has a valid connection. The Diameter protocol allows only one connection from a particular peer.

Note: This situation only occurs when `DIAMETER.AllowMultipleConnectionsPerPeer` is set to false, or when the multiple connections setting is turned off on the Advanced Settings of the Policy Server tab in the CMP system.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 300 seconds.

OID

DIAMETERNewConnRejected

Recovery:

1. Check the peer configuration and ensure that the peer sees a valid connection with the device.
2. If the problem persists, contact [My Oracle Support](#).

71414 – SCTP Path Status Changed

Alarm Type

PCRF

Description

SCTP Path Status Changed. Occurs when an MPE or MRA device is multihoming. The alarm occurs when one path fails, and clears when the path becomes available again. If the path that is currently transmitting Diameter messages fails, the alarm is triggered when the SCTP association tries to send the next Diameter message. If the path is not transmitting Diameter messages (it is a backup) then it may take up to 30 seconds for the alarm to be triggered, since heartbeat chunks are sent every 30 seconds.

Default Severity

Minor

Instance

Peer address + Association ID

HA Score

Normal

Clearing Action

This alarm clears automatically after 7200 seconds (2 hours).

OID

SctpPathStatusChanged

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

71605 – LDAP Conn Failed

Alarm Type

PCRF

Description

Connection to LDAP server failed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to LDAP server is restored or clears automatically after 7200 seconds (2 hours).

OID

LdapConnFailed

Recovery:

1. Verify that there is no problem with the LDAP server or the network path used to reach the server.
2. If the problem persists, contact [My Oracle Support](#).

71630 – DHCP Unexpected Event ID**Alarm Type**

PCRF

Description

DHCP Communication exception.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Next successful DHCP operation will clear this alarm.

OID

DHCPUnexpectedEventId

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

71631 – DHCP Unable to Bind Event ID**Alarm Type**

PCRF

Description

DHCP unable to bind event ID.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Next successful DHCP bind operation will clear this alarm or clears automatically after 60 seconds.

OID

DHCPUnableToBindEventId

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

71632 – DHCP Response Timeout Event ID

Alarm Type

PCRF

Description

DHCP Response Timeout Event Id.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 seconds.

OID

DHCPResponseTimeoutEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

71633 – DHCP Bad Relay Address Event ID

Alarm Type

PCRF

Description

DHCP bad relay address event id.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 30 seconds.

OID

DHCPBadRelayAddressEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

71634 – DHCP Bad Primary Address Event ID**Alarm Type**

PCRF

Description

DHCP no primary address specified.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 30 seconds.

OID

DHCPBadPrimaryAddressEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

71635 – DHCP Bad Secondary Address Event ID**Alarm Type**

PCRF

Description

DHCP no secondary address specified.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 30 seconds.

OID

DHCPBadSecondaryAddressEventId

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

71684 – SPR Connection Closed

Alarm Type

PCRF

Description

SPR Closing a secondary connection to revert to primary connection.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to SPR is restored.

OID

SPRConnectionClosed

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

71685 – MSR DB Not Reachable

Alarm Type

PCRF

Description

Unable to connect to Multimedia Subscriber Repository (MSR) after several attempts.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to MSR is restored.

OID

MSRDBNotReachable

Recovery:

1. Verify that there is no problem with the MSR server or the network path used to reach the server.
2. If the problem persists, contact [My Oracle Support](#).

71702 – BRAS Connection Closed

Alarm Type

PCRF

Description

BRAS Connection Closed. The MPE device lost a connection to the B-RAS element of the gateway.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to BRAS is restored.

OID

BrasConnectionClosed

Recovery:

1. Check availability of the gateway.
2. If the gateway has not failed, make sure that the path from the gateway to the MPE is operational.

3. If the problem persists, contact [My Oracle Support](#).

71703 – COPS Unknown Gateway

Alarm Type

PCRF

Description

COPS Unknown Gateway. An unknown gateway is trying to establish a COPS-PR connection to the MPE device.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

COPS network element is associated with MPE device.

OID

COPSUnknownGateway

Recovery:

1. Check the configuration of the network elements in the CMP system. There should be a B-RAS network element for this gateway and that B-RAS must be associated with this MPE device.
2. Make sure that the configuration of the B-RAS network element is consistent with the provisioned information on the gateway.

The network element name in the CMP system must match the provisioned router name on the gateway.

3. If the problem persists, contact [My Oracle Support](#).

71801 – PCMM No PCEF

Alarm Type

PCRF

Description

This alarm is raised when the MPE cannot find the PCEF. The alarm is disabled by default unless the user sets `RC.TrapNoPcefEnabled` to true in `RcMgr`. This update occurs in both the MPE-R and MPE-S. The `SubId` in the alarm details is actually `CMTSIP` if the MPE uses `CMTSIP` to find PCEF when it receives PCMM requests. The PCMM requests may be `GateSet/GateInfo/GateDelete`.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 seconds.

OID

PCMMNoPCEF

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

71805 – PCMM Non Connection PCEF**Alarm Type**

PCRF

Description

PCMM Non Connection to PCEF.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 seconds.

OID

PCMMNonConnectionPCEF

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

72198 – SMSR SMSC Switched to Primary**Alarm Type**

PCRF

Description

Switched to primary Short Message Service Center (SMSC). Switched from Secondary to Primary SMSC.

Default Severity

Minor

Instance

SMSC address

HA Score

Normal

Clearing Action

This alarm automatically clears after 60 minutes (3600 seconds).

OID

SMSRSMSCSwitchedToPrimary

Recovery:

1. No action necessary.

72199 – SMSR SMSC Switched to Secondary

Alarm Type

PCRF

Description

Switched to Secondary Short Message Service Center (SMSC). Switched from Primary to Secondary SMSC.

Default Severity

Minor

Instance

SMSC Address

HA Score

Normal

Clearing Action

This alarm automatically clears after 60 minutes (3600 seconds).

OID

SMSRSMSCSwitchedToSecondary

Recovery:

1. No action necessary.

72210 – PCMM Reached Max Gates Event ID

Alarm Type

PCRF

Description

PCMM Reached Maximum Gates. A subscriber at IP address *ip-addr* has reached the configured maximum number of upstream gates.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 seconds.

OID

PCMMReachedMaxGatesEventId

Recovery:

1. If this alarm occurs infrequently, monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

72211 – PCMM Reached Max GPI Event ID**Alarm Type**

PCRF

DescriptionPCMM Reached Maximum GPI. A subscriber at IP address *ip-addr* has reached the configured maximum grants per interval on all upstream gates.**Default Severity**

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 seconds.

OID

PCMMReachedMaxGPIEventId

Recovery:

1. This subscriber address is exceeding the capacity; attention is required.
2. If the problem persists, contact [My Oracle Support](#).

72501 – SCE Connection Lost**Alarm Type**

PCRF

Description

Service Control Engine (SCE) Connection is lost.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Connection to SCE is restored.

OID

SCEConnectionLost

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

72549 – SMSR Queue Full

Alarm Type

PCRF

Description

Short Message Service Relay (SMSR) internal queue is full: notification internal queue has reached capacity. Messages will be rejected until the queue space becomes available.

Default Severity

Minor

Instance

SMSR queue

HA Score

Normal

Clearing Action

Available capacity is restored and queue begins to accept new messages or automatically clears after 60 minutes (3600 seconds).

OID

SMSRQueueFull

Recovery:

1. Check configuration and availability of the destination service to ensure there are no connections problems and that the network path from the MPE device to the element (host/port/resource location) is operational.

72559 – SMSR SMSC Connection Closed

Alarm Type

PCRF

Description

SMSC connection closed.

Default Severity

Minor

Instance

SMSC address

HA Score

Normal

Clearing Action

This alarm automatically clears after 60 minutes (3600 seconds) or when the SMSC connection is restored.

OID

SMSRSMSCConnectionClosed

Recovery:

1. No action necessary.

72565 – SMSR SMTP Connection Closed

Alarm Type

PCRF

Description

Simple Mail Transfer Protocol (SMTP) connection closed. SMTP connection has been closed to MTA *{IP Address}*.

Default Severity

Minor

Instance*{host name of MTA}***HA Score**

Normal

Clearing Action

This alarm automatically clears after 60 minutes (3600 seconds) or when the SMTP connection is restored.

OID

SMSRSMTPConnectionClosed

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

72575 – Policy Notification:Lost connection with destination URL

Alarm Type

PCRF

Description

The connection to a configured Policy Notification destination was lost.

Default Severity

Minor

Instance

Destination Name

HA Score

Normal

Clearing Action

Auto clears after 60 minutes (3600 seconds) or when HTTP connection is restored.

OID

SMSRHTTPConnectionClosed

Recovery:

1. Check configuration, including URL, and availability of the destination service.
2. Check the client for reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (host/port/resource location) is operational.
4. If the problem persists, contact [My Oracle Support](#).

72703 – RADIUS Server Failed

Alarm Type

PCRF

Description

RADIUS server start failed.

Default Severity

Minor

Instance

N/A

HA Score

N/A

Clearing Action

N/A

OID

RADIUSServerFailed

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

72706 - RADIUS Server Corrupt Auth**Alarm Type**

PCRF

Description

RADIUS authenticator is corrupted.

Severity

Minor

Instance

N/A

HA Score

N/A

Clearing Action

N/A

OID

RADIUServerCorrupAuth

Recovery:

1. Check the connectivity and configuration of the RADIUS server.

72904 – Diameter Too Busy**Alarm Type**

PCRF

Description

System has entered a busy state.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

The Diameter load drops below admission criteria thresholds or this alarm clears automatically after 30 seconds.

OID

DiameterTooBusy

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

72905 – Radius Too Busy

Alarm Type

PCRF

Description

RADIUS load shedding set a busy state.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

The RADIUS load drops below admission criteria thresholds or this alarm clears automatically after 30 seconds.

OID

RadiusTooBusy

Recovery:

1. If this alarm occurs infrequently, then monitor the health of the system.
2. If this alarm occurs frequently, contact [My Oracle Support](#).

74000 – Policy Server Critical Alarm

Alarm Type

PCRF

Description

Critical Policy alarm.

Default Severity

Critical

Instance

N/A

HA Score

Normal

Clearing Action

This alarm can be cleared by a policy or clears automatically after 3600 seconds (60 minutes).

OID

PolicyServerCriticalAlarm

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

74001 – Policy Server Major Alarm

Alarm Type

PCRF

Description

Major Policy alarm.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm can be cleared by a policy or clears automatically after 3600 seconds (60 minutes).

OID

PolicyServerMajorAlarm

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

74002 – Policy Server Minor Alarm

Alarm Type

PCRF

Description

Minor Policy alarm.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm can be cleared by a policy or clears automatically after 3600 seconds (60 minutes).

OID

PolicyServerMinorAlarm

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

74020 – Stats Files Generator Delete Expire Files

Alarm Type

PCRF

Description

Delete expire files. Stats Files Generator Task has removed some files which were not synchronized to remote servers (*{external system IP}, {external system IP}, etc*).

Default Severity

Major

Instance

Stats files generator

HA Score

Normal

Clearing Action

The alarm is automatically cleared after 300 seconds (5 minutes).

OID

StatsFilesGeneratorDeleteExpireFiles

Recovery:

1. Check all enabled Stats Files Synchronization tasks status in the DC (Data Collection) tasks of CMP system and ensure they are configured successfully.
2. Exchange SSL key with mate server in cluster.

74021 – Files Synchronization Failure

Alarm Type

PCRF

Description

Files synchronization failure. Files Synchronization #{num} task failed to synchronize local to remote server (*external system Host Name/IP*) after retry {num} times, where:

- {num} is task #
- {num} is retry times (1 to 5)
- *external system Host Name/IP* is the user-defined remote server's IP address to which files are synchronized

Default Severity

Minor

Instance

Stats files synchronization

HA Score

Normal

Clearing Action

Auto clear 300 seconds

OID

FilesSynchronizationFailure

Recovery:

1. Check the network status of the remote server which you configured in the Stats Files Synchronization task.
2. Ensure remote server supports SSH protocol and you configured the user name and password correctly.

74022 - Files Uploading Failure

Alarm Type

PCRF

Description

PM Statistics Files Uploading Task failed to upload local statistics files to FTP server *FTP server Host Name/IP* after retry *number* times.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm automatically clears after 5 minutes (300 seconds).

OID

FilesUploadingFailureNotify

Recovery:

1. Fix network problems or verify FTP configuration information, which is defined in the scheduler task of the CMP system.
2. If the issue does not resolve, contact [My Oracle Support](#).

74102 - CMTS Subnet Overlapped

Alarm Type

Description

Overlapped subnets are present on the CMTS.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Auto clears when task runs again.

OID

CmtsSubnetOverlapped

Recovery:

1. Go to Schedule Tasks Administration with menu item **System Administration > Scheduled Tasks**.
2. Open Subnet Overlap Detector Task hyperlink.
3. Open Subnet Overlapping Report by clicking 'details' hyperlink in Exit Status Message.
4. Refer to Subnet Overlap Report for overlapped subnets of CMTS detail information.
5. Reconfigure the subnets of CMTS to resolve the overlap.
6. Run the Subnet Overlap Detector task again.
7. If the issue still exists, repeat the previous steps.

74103 - NES Without CMTS IP

Alarm Type

Description

This alarm is raised when Routing by CMTS IP is enabled and Network Elements exist without CMTS IP addresses assigned.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm automatically clears after 30 seconds.

OID

NeWithoutCmtsIp

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

74602 - Multiple Active In Cluster Failure

Alarm Type

QP

Description

Multiple Active servers have been detected in the same cluster; the cluster is in Split Brain state.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears when HA recovers or clears automatically after 30 minutes (1800 seconds). When HA recovers there will be only one Active server in a cluster.

OID

QPMultipleActiveInClusterFailure

Recovery:

1. Fix network problems and restore connectivity.
2. Place one of the Active servers in the cluster into Forced Standby mode.
3. If the problem persists, contact [My Oracle Support](#).

74603 - Max Primary Cluster Failure Threshold

Alarm Type

QP

Description

The number of failed MPE pairs reaches the threshold of *configured threshold value* at *site name*.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears when the number of failed MPE pairs remain at a lower value than the threshold of *max primary site failure threshold* at *site*, or clears automatically after 30 minutes (1800 seconds).

OID

QPMaxMPEPrimaryClusterFailure

Recovery:

1. When the failure count drops below the threshold value and stays below the threshold for 30 seconds, the alarm is cleared. (The 30 seconds delay prevents the alarm from being cleared too soon.)
2. If alarm does not clear automatically, contact [My Oracle Support](#).

74604 - MPE Cluster Offline Failure

Alarm Type

QP

Description

Policy Cluster is offline.

Default Severity

Critical

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears when a server in the MPE cluster comes online. The alarm clears automatically after 30 minutes (1800 seconds).

OID
QPMPEClusterOfflineFailure

Recovery:

1. When a server comes online (in Active, Standby, or Spare state), the alarm is cleared. Please check whether all servers are powered down or rebooted at that time.
2. If alarm does not clear automatically, contact [My Oracle Support](#).

74605 - Subscriber Trace Backup Failure

Alarm Type
QP

Description
The script responsible for backing up the subscriber trace log has failed.

Default Severity
Minor

Instance
N/A

HA Score
Normal

Clearing Action

OID
SubscriberTraceBackupFailure

Recovery:

1. When a server comes online (in Active, Standby, or Spare state), the alarm is cleared. Please check whether all servers are powered down or rebooted at that time.
2. If alarm does not clear automatically, contact [My Oracle Support](#).

75000 - Policy Library Loading Failed

Alarm Type
PCRF

Description
Policy library loading failed. PCRF was unable to load the latest policy library. If this alarm occurred at startup time or at failover, this indicates the PCRF does not have any policies deployed. If this alarm occurred on a new policy push when PCRF was running with some existing policies, this alarm indicates that the PCRF will continue to run with those existing policies.

Default Severity
Major

Instance

N/A

HA Score

Normal

Clearing Action

Performing a reapply config may fix the problem.

OID

PolicyLoadingLibraryFailed

Recovery:

1. Perform a reapply config from the CMP system to reload the library.
2. If the problem persists, contact [My Oracle Support](#).

77904 - BOD PCMM Too Busy

Alarm Type

PCRF

Description

BOD PCMM load shedding set a busy state.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 30 seconds.

OID

BODPCMMTooBusy

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

77905 - BOD DIAMETER Too Busy

Alarm Type

PCRF

Description

BOD DIAMETER Too Busy

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 30 seconds.

OID

BODDiameterTooBusy

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

78000 - ADS Connection Lost

Alarm Type

PCRF

Description

ADS Connection Lost. The Analytics Data Stream (ADS) connection was lost to the specified client.

Default Severity

Minor

Instance

Analytics Client ID

HA Score

Normal

Clearing Action

Connection to a remote peer is restored by the same client (ID), or automatically clears in 60 minutes (3600 seconds).

OID

ADSConnectionLost

Recovery:

1. Check configuration and availability of the analytics client.
2. Check the client for reboot or other service interruption.
3. If the element has not failed, make sure that the network path from the MPE device to the element (port 222) is operational.
4. If the problem persists, contact [My Oracle Support](#).

78001 - Rsync Failed

Alarm Type

PCRF

Description

Transfer of Policy jar files failed. PCRFB was unable to transfer the latest policy library from the active to the standby server. The alarm can be raised by the active server when a policy change is made or a Reapply Configuration is performed. It can be raised by the standby server during startup if it was unable to get the policy jar file from the active server during startup.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

Since the alarm can be raised by both the active and standby servers, the alarm will not clear once the problem is fixed. It will be cleared when the issue is fixed internally on the affected blades.

OID

RsyncFailed

Recovery:

1. This alarm can be ignored during a mixed version upgrade (for example, 7.5/7.6 to 9.1) and when rebooting both servers on the MPE device.
2. If the alarm is seen on the MRA device, it indicates the logback config files are not transferring, which is harmless to the operation.
3. The most likely cause is that the ssh keys have not been exchanged; ensure they are exchanged correctly.
4. Perform a Reapply Configuration.
5. If performing a Reapply Configuration does not fix the problem, another alarm will be raised by the active server for that particular operation. If the problem persists, contact [My Oracle Support](#).

78850 - VNF operation error

Alarm Type

PCRFB

Description

There was an error while performing the requested operation on the VNF cluster.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

The event will clear when the VM is in the Active state or the event must be cleared manually.

OID

VNFOperationError

Recovery:

1. Trace Logs provide details of the operation failure and which VMs were impacted. Validate information that was submitted as part of the request. Correct Topology and repeat the failed operation or take corrective action on the VM directly.

79002 - Sess Size Reached Threshold**Alarm Type**

PCRF

Description

Total session database size reached maximum threshold percentage of planned session database size.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Total session database size goes below minimum threshold percentage of planned session database size.

OID

SessDBSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the expectation.
2. If the problem persists, contact [My Oracle Support](#).

79003 - Avg Sess Size Exceed**Alarm Type**

PCRF

Description

Average session size exceeded the projected size.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 minutes (3600 seconds).

OID

AvgSessSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the customer's expectation.
2. If the problem persists, contact [My Oracle Support](#).

79004 - Bind Size Reached Threshold

Alarm Type

PCRF

Description

Total binding database size reached maximum threshold percentage of planned binding database size.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

Total binding database size goes below minimum threshold percentage of planned binding database size or clears automatically after 60 minutes (3600 seconds).

OID

BindDBSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the customer's expectation.
2. If the problem persists, contact [My Oracle Support](#).

79005 - Avg Bind Size Exceed

Alarm Type

PCRF

Description

Average binding size exceeded the projected size.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 60 minutes (3600 seconds).

OID

AvgBindSizeReachedThreshold

Recovery:

1. Check the threshold configuration to make sure that it matches the expectation.
2. If the problem persists, contact [My Oracle Support](#).

79105 - Mediation SOAP Too Busy

Alarm Type

PCRF

Description

Mediation Server SOAP provisioning interface reaches busy state; load shedding begins.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 30 seconds or when the Mediation load recovers.

OID

MediationSOAPTTooBusy

Recovery:

1. Check that UDR is in a normal state to handle a SOAP provisioning request.
2. If the problem persists, contact [My Oracle Support](#).

79106 - SPR Connection Failed

Alarm Type

PCRF

Description

Created connection to SPR failed.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears when provisioning the connection between the Mediation and UDR recovers.

OID

SPRConnectionFailed

Recovery:

1. Check that the provisioning data source configuration on the Mediation server is correct.
2. If the problem persists, contact [My Oracle Support](#).

79107 - Mediation Disk Quota Exceed

Alarm Type

PCRF

Description

Sync directory disk quota exceeded.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 3600 seconds or when the disk usage of the Mediation server is decreased to value less than the quota limit.

OID

MSDiskQuotaExceed

Recovery:

1. Release disk usage to ensure that 32G of free disk space is available in the sync directory.
2. If the problem persists, contact [My Oracle Support](#).

79108 - Mediation Disk No Space**Alarm Type**

PCRF

Description

No space left on device.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears when the disk space is not fully used.

OID

MSDiskNoSpace

Recovery:

1. Release disk usage to ensure that 32G of free disk space is available in the sync directory.
2. If the problem persists, contact [My Oracle Support](#).

79109 - SPR License Limit**Alarm Type**

PCRF

Description

Achieve 80% maximum number of users in SPR.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

SPRLicenseLimit

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

79110 - Files Uploading Failure

Alarm Type

PCRF

Description

SMS Notification Statistics Upload Task failed to upload stats files to remote FTP server after retry.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

Auto clears after 300 seconds or the next time the task is run.

OID

FilesUploadingFailure

Recovery:

1. Check the FTP server configuration is correct in schedule task *SMS Notification Statistics Uploading Task*.
2. Check and ensure remote FTP server is accessible and service is available.

79120 - Batch Disk Quota Exceeds

Alarm Type

PCRF

Description

The batch folder disk quota exceeds.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

BatchDiskQuotaExceeds

Recovery:

1. If the problem persists, contact [My Oracle Support](#).

79995 - X1 Connection Lost**Alarm Type**

PCRF

Description

The X1 Connection between the Mediation Function and Policy Server is Lost.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 7200 seconds.

OID

X1ConnectionLost

Recovery:

1. Check if the X1 Connection is down.
2. If the problem persists, contact [My Oracle Support](#).

79996 - X2 Connection Lost**Alarm Type**

PCRF

Description

X2 Connection between the Policy Server and Mediation Function is Lost.

Default Severity

Minor

Instance

N/A

HA Score

Normal

Clearing Action

This alarm clears automatically after 7200 seconds.

OID

X2ConnectionLost

Recovery:

1. Check if the X2 Connection is down.
2. If the problem persists, contact [My Oracle Support](#).

Policy Server Events (80000-89999)

This section provides a list of Policy Server events (80000-89999) which are generated by policy devices, such as MPE devices and MRA devices.

80001 - DB State Transition

Alarm Type

QP

Description

The DB status of the blade is not fully ready. The MySQL database manager generates a "MySQL state transition" event every time it makes a state-machine transition. The event text describes the transition.

Default Severity

Info

Instance

MySQL

HA Score

Normal

Clearing Action

This alarm is cleared by `qp-procmgr` as `qp-procmgr` shuts down.

OID

QPDBStateChange

Recovery:

1. Because this is an information-only message, there is no recovery action required.

80002 - MySQL Relay Log Dropped

Alarm Type

QP

Description

A portion of the MySQL relay log was dropped as the secondary server was shutting down. This event is raised when a secondary server times out while trying to apply its relay log during a secondary stop. The server may not be hurt, but there may be after effects. This event is raised to trigger a debug for possible after effects.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

QPMySQLRelayLogDropped

Recovery:

1. Debug the system for possible after effects caused by the timeout.

80003 - QP MySQL DB Level

Alarm Type

QP

Description

The ranking of secondaries when the primary database is outdated. If the primary database is outdated, the server raises this event once per minute. The server will rank the secondaries, from best to worst, based on their database level.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

QPMySQLDBLevel

Recovery:

1. Use the information of this event to help resolve an outdated primary database raised by alarm 70020.

82704 - Binding Release Task

Alarm Type

PCRF

Description

Binding Release Task. The binding release task has started, completed, or aborted.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

BindingReleaseTask

Recovery:

1. No action required.

84004 - Policy Info Event

Alarm Type

PCRF

Description

Policy Info Event. Application is ready.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

PolicyInfoEvent

Recovery:

1. No action required.

86001 – Application Is Ready

Alarm Type

PCRF

Description

Application is ready for service.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

ApplicationIsReady

Recovery:

1. No action required.

86100 - CMP User Login

Alarm Type

PCRF

Description

CMP user login was successful.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMPLUserLogin

Recovery:

1. No action required. Recovery is immediate.

86101 - CMP User Login Failed

Alarm Type

PCRF

Description

CMP user login failed.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMPUserLoginFailed

Recovery:

1. No action required. Recovery is immediate.

86102 - CMP User Logout

Alarm Type

PCRF

Description

CMP User performed logout.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMPUserLogout

Recovery:

1. No action required. Recovery is immediate.

86200 - CMP User Promoted Server

Alarm Type

PCRF

Description

CMP user promoted server. The current site becomes the Primary site.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMUserPromotedServer

Recovery:

1. No action required. Recovery is immediate.

86201 - CMP User Demoted Server

Alarm Type

PCRF

Description

CMP user demoted server. The current site becomes the Secondary site.

Default Severity

Info

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMUserDemotedServer

Recovery:

1. No action required. Recovery is immediate.

86300 - Sh Enable Failed

Alarm Type

PCRF

Description

Enable Sh Connection failed. The CMP server performed a global operation to enable Sh on all MPE devices and it failed on the specified MPE.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMPSHConEnableFailed

Recovery:

1. The operation can be retried. If repeated attempts fail, there may be other management issues with the associated MPE devices and connectivity to those devices should be verified.

86301 - Sh Disable Failed

Alarm Type

PCRF

Description

Disable Sh Connection failed. The CMP performed a global operation to disable Sh on all MPE devices and it failed on the specified MPE.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID
CMPShConDisableFailed

Recovery:

1. The operation can be retried. If repeated attempts fail, there may be other management issues with the associated MPE devices and connectivity to those devices should be verified.

86303 - NW-CMP Apply Failed

Alarm Type
PCRF

Description
NW-CMP failed to apply settings to S-CMP.

Default Severity
Major

Instance
N/A

HA Score
Normal

Clearing Action
N/A

OID
NWCMPApplyFailed

Recovery:

1. The alarm on the NW-CMP will be cleared once the NW-CMP successfully applies the configuration to the S-CMP.

86304 - S-CMP Unreachable

Alarm Type
PCRF

Description
The S-CMP is offline or unreachable by the NW-CMP. This alarm will be raised on the NW-CMP.

Default Severity
Major

Instance
N/A

HA Score
Normal

Clearing Action

N/A

OID

SCMPUNREACHABLE

Recovery:

1. This alarm will be cleared once the S-CMP is reachable.

86305 - S-CMP Split Brain

Alarm Type

PCRF

Description

When a geo-redundant S-CMP is in split brain (that is, both sites are reporting as Primary), an alarm is raised on NW-CMP.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

SCMPSplitBrain

Recovery:

1. This alarm will be cleared automatically when the split brain on the S-CMP is gone.

86306 - CMP Apply Failed

Alarm Type

PCRF

Description

When a CMP system failed to apply settings to any MRA or MPE device, this alarm is raised on this S-CMP.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

CMPApplyFailed

Recovery:

1. This alarm will be cleared automatically when the next applying to that MRA or MPE device is successful.

86307 - S-CMP Sync Fails**Alarm Type**

PCRF

Description

If the connection between the NW-CMP and the S-CMP is broken and the synchronization fails, an alarm will be raise in S-CMP.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

SCMPSYNCFAILS

Recovery:

1. The alarm will be cleared once the synchronization is successful in the next cycle.

86308 - NCMP Ref Obj Miss**Alarm Type**

PCRF

Description

The top level object is missing in NW-CMP but is referred by S-CMP server. This alarm will be raised in the NW-CMP server.

Default Severity

Major

Instance

N/A

HA Score

Normal

Clearing Action

N/A

OID

NCMPReferdObjMiss

Recovery:

1. This alarm will be cleared once there is no referred but missing top level object.