Oracle® Communications Diameter Signaling Router

Alarms and KPIs

Release 8.5.0.1
F37854-02
May 2021

ORACLE

Oracle Communications Diameter Signaling Router Alarms and KPIs, Release 8.5.0.1

F37854-02

Copyright © 2011, 2021, Oracle and/or its affiliates.

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 embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. 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 Inside 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, Epyc, and the AMD 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

1 Introduction

Revision History 1-1
Overview 1-1
Scope and Audience 1-2
Manual Organization 1-2
My Oracle Support 1-2

2 Alarms, Events, and KPIs Overview

Alarms Warning 2-1
General alarms and events information 2-1
- Alarms and Events Overview 2-1
- Alarms Formatting Information 2-3
- Alarm and Event ID Ranges 2-4
- Alarm and Event Types 2-4
- Active Alarms Elements 2-6
- View Active Alarms 2-7
- Active Alarms Data Export Elements 2-7
- Export Active Alarms 2-9
- Generate a Report of Active Alarms 2-10
- Graph Active Alarms 2-11
- Active Alarms Quick Filter 2-11
- Viewing alarm and event history 2-12
- Historical events data export elements 2-13
- Exporting alarm and event history 2-14
- Generating a report of historical alarms and events 2-15

View the File List 2-16
Opening a File 2-16
Data Export 2-16
- Data Export elements 2-16
- Configuring data export 2-18

Tasks 2-19
- Active Tasks 2-19

Active Tasks elements 2-20
Deleting a task 2-20
Deleting all completed tasks 2-21
Cancelling a running or paused task 2-21
Pausing a task 2-21
Restarting a task 2-22
Active Tasks report elements 2-22
Generating an active task report 2-23
Scheduled Tasks 2-23
Scheduled Tasks Elements 2-24
Editing a Scheduled Task 2-24
Deleting a Scheduled Task 2-24
Generating a Scheduled Task Report 2-24

3 Alarms and Events

IP Front End, IPFE (5000-5999) 3-1
5001 - IPFE Backend Unavailable 3-1
5002 - IPFE Address Configuration Error 3-2
5003 - IPFE State Sync Run Error 3-4
5004 - IPFE IP Tables Configuration Error 3-7
5005 - IPFE Backend In Stasis 3-8
5006 - Error Reading from Ethernet Device. Restart IPFE Process. 3-10
5007 - Out of Balance: Low 3-10
5008 - Out of Balance: High 3-12
5009 - No Available Servers in Target Set 3-13
5010 - Unknown Linux iptables Command Error 3-16
5011 - System or Platform Error Prohibiting Operation 3-17
5012 - Signaling Interface Heartbeat Timeout 3-18
5013 - Throttling Traffic 3-19
5100 - Traffic Overload 3-21
5101 - CPU Overload 3-23
5102 - Disk Becoming Full 3-23
5103 - Memory Overload 3-24
OAM (10000-10999) 3-24
10001 - Database Backup Started 3-24
10002 - Database Backup Completed 3-25
10003 - Database Backup Failed 3-25
10004 - Database Restoration Started 3-26
10005 - Database Restoration Completed 3-26
10006 - Database Restoration Failed 3-27

10008 - Database Provisioning Manually Disabled 3-27
10009 - Config and Prov DB Not Yet Synchronized 3-28
10010 - Stateful DB from Mate Not Yet Synchronized 3-29
10011 - Cannot Monitor Table 3-29
10012 - Table Change Responder Failed 3-30
10013 - Application Restart in Progress 3-30
10020 - Backup Failure 3-31
10050 - Resource Audit Failure 3-31
10051 - Route Deployment Failed 3-32
10052 - Route Discovery Failed 3-33
10053 - Route Deployment Failed - No Available Device 3-33
10054 - Device Deployment Failed 3-34
10055 - Device Discovery Failed 3-35
10073 - Server Group Max Allowed HA Role Warning 3-36
10074 - Standby Server Degraded While Mate Server Stabilizes 3-37
10075 - Application Processes Have Been Manually Stopped 3-37
10078 - Application Not Restarted on Standby Server Due to Disabled Failure Cleanup Mode 3-38
10100 - Log Export Started 3-38
10101 - Log Export Successful 3-39
10102 - Log Export Failed 3-39
10103 - Log Export Already in Progress 3-40
10104 - Log Export File Transfer Failed 3-40
10105 - Log Export Cancelled - User Request 3-41
10106 - Log Export Cancelled - Duplicate Request 3-42
10107 - Log Export Cancelled - Queue Full 3-42
10108 - Duplicate Scheduled Log Export Task 3-43
10109 - Log Export Queue is Full 3-44
10110 - Certificate About to Expire 3-44
10111 - Certificate Expired 3-46
10112 - Certificate Cannot be Used 3-47
10115 - Health Check Started 3-49
10116 - Health Check Successful 3-49
10117 - Health Check Failed 3-50
10118 - Health Check Not Run 3-50
10120 - Server Group Upgrade Started 3-51
10121 - Server Group Upgrade Cancelled - Validation Failed 3-51
10122 - Server Group Upgrade Successful 3-52
10123 - Server Group Upgrade Failed 3-52
10124 - Server Group Upgrade Cancelled - User Request 3-53
10125 - Server Group Upgrade Failed 3-53

10130 - Server Upgrade Started 3-54
10131 - Server Upgrade Cancelled 3-54
10132 - Server Upgrade Successful 3-55
10133 - Server Upgrade Failed 3-55
10134 - Server Upgrade Failed 3-56
10140 - Site Upgrade Started 3-58
10141 - Site Upgrade Cancelled 3-59
10142 - Site Upgrade Successful 3-59
10143 - Site Upgrade Failed 3-60
10144 - Site Upgrade Cancelled - User Request 3-60
10145 - Site Upgrade Failed 3-61
10151 - Login Successful 3-61
10152 - Login Failed 3-62
10153 - Logout Successful 3-62
10154 - User Account Disabled 3-63
10155 - SAML Login Successful 3-63
10156 - SAML Login Failed 3-64
10200 - Remote Database Reinitialization in Progress 3-64
10300 - SNMP Trapping Not Configured 3-65
IDIH (11500-11549) 3-65
11500 - Tracing Suspended 3-65
11501 - Trace Throttling Active 3-66
11502 - Troubleshooting Trace Started 3-66
11503 - Troubleshooting Trace Stopped 3-67
11506 - Invalid IDIH-Trace AVP 3-67
11507 - Unable to Run Network Trace at This Site 3-68
11508 - Network Trace Configuration Error 3-68
11509 - Site Trace Configuration Error 3-69
11510 - Network Trace Activation Error 3-69
11511 - Invalid DIH HostName 3-70
SDS (14000-14999) 3-70
14100 - Interface Disabled 3-71
14101 - No Remote Connections 3-71
14102 - Connection Failed 3-72
14103 - Both Port Identical 3-72
14120 - Connection Established 3-73
14121 - Connection Terminated 3-73
14122 - Connection Denied 3-74
14140 - Import Throttled 3-74
14150 - Import Initialization Failed 3-75
14151 - Import Generation Failed 3-75

14152 - Import Transfer Failed 3-76
14153 - Export Initialization Failed 3-76
14154 - Export Generation Failed 3-77
14155 - Export Transfer Failed 3-77
14160 - Import Operation Completed 3-78
14161 - Export Operation Completed 3-78
14170 - Remote Audit Started and In Progress 3-79
14171 - Remote Audit Aborted 3-79
14172 - Remote Audit Failed to Complete 3-80
14173 - Remote Audit Completed 3-80
14174 - NPA Split Pending Request Deleted 3-81
14175 - NPA Split Activation Failed 3-81
14176 - NPA Split Started and Is Active 3-82
14177 - NPA Split Completion Failed 3-82
14178 - NPA Split Completed 3-83
14179 - MSISDN Deleted From Blacklist 3-83
14180 - IMSI Deleted from Blacklist 3-84
14188 - PdbRelay Not Connected 3-84
14189 - PdbRelay Time Lag 3-85
14198 - ProvDbException 3-85
14200 - DP Stack Event Queue Utilization 3-86
14301- ERA Responder Failed 3-87
SS7/Sigtran (19200-19299) 3-87
19200 - RSP/Destination Unavailable 3-87
19201 - RSP/Destination Route Unavailable 3-88
19202 - Linkset Unavailable 3-89
19203 - Link Unavailable 3-90
19204 - Preferred Route Unavailable 3-90
19205 - TFP Received 3-91
19206 - TFA Received 3-92
19207 - TFR Received 3-92
19208 - TFC Received 3-93
19209 - M3RL Routing Error 3-93
19210 - M3RL Routing Error - Invalid NI 3-94
19211 - M3RL Routing Error - Invalid SI 3-95
19217 - Node Isolated - All Links Down 3-96
19226 - Timed Out Waiting for ASP-UP-ACK 3-96
19227 - Received Unsolicited ASP-DOWN-ACK 3-97
19229 - Timed Out Waiting for ASP-ACTIVE-ACK 3-98
19230 - Received Unsolicited ASP-INACTIVE-ACK 3-98
19231 - Received Invalid M3UA Message 3-99

19233 - Failed to Send Non-DATA Message 3-100
19234 - Local Link Maintenance State Change 3-101
19235 - Received M3UA Error 3-101
19240 - Remote SCCP Subsystem Prohibited 3-103
19241 - SCCP Malformed or Unsupported Message 3-104
19242 - SCCP Hop Counter Violation 3-104
19243 - SCCP Routing Failure 3-105
19244 - SCCP Routing Failure Network Status 3-106
19245 - SCCP GTT Failure 3-107
19246 - Local SCCP Subsystem Prohibited 3-107
19248 - SCCP Segmentation Failure 3-108
19249 - SCCP Reassembly Failure 3-109
19250 - SS7 Process CPU Utilization 3-109
19251 - Ingress Message Rate 3-110
19252 - PDU Buffer Pool Utilization 3-111
19253 - SCCP Stack Event Queue Utilization 3-112
19254 - M3RL Stack Event Queue Utilization 3-113
19255 - M3RL Network Management Event Queue Utilization 3-114
19256 - M3UA Stack Event Queue Utilization 3-114
19258 - SCTP Aggregate Egress Queue Utilization 3-115
19259 - Operation Discarded Due to Local Resource Limitation 3-116
19260 - Transaction Could Not be Delivered to Remote TCAP Peer Due to Conditions in the Network 3-117
19262 - Operation Discarded Due to Malformed Component Received from Remote TCAP Peer 3-117
19263 - Transaction Discarded Due to Malformed Dialogue Message Received from Local TC User 3-118
19264 - Transaction Discarded Due to Malformed Dialogue Message from Remote TCAP Peer 3-119
19265 - Unexpected Event Received from Local TC User 3-119
19266 - Unexpected Event Received from Remote TCAP Peer 3-120
19267 - Dialogue Removed by Dialogue Cleanup Timer 3-121
19268 - Operation Removed by Invocation Timer Expiry 3-121
19269 - Dialogue Aborted by Remote TCAP Peer 3-122
19270 - Received Unsupported TCAP Message 3-123
19271 - Operation Rejected by Remote TCAP Peer 3-124
19272 - TCAP Active Dialogue Utilization 3-124
19273 - TCAP Active Operation Utilization 3-125
19274 - TCAP Stack Event Queue Utilization 3-126
19275 - Return Error from Remote TCAP Peer 3-126
19276 - SCCP Egress Message Rate 3-127
19281 - TCAP Routing Failure 3-128

Transport Manager (19400-19419) 3-128
19400 - Transport Down 3-128
19401 - Failed to Configure Transport 3-130
19402 - Failed to Connect Transport 3-130
19403 - Received Malformed SCTP Message (Invalid Length) 3-131
19404 - Far-End Closed the Transport 3-132
19405 - Transport Closed Due to Lack of Response 3-133
19406 - Local Transport Maintenance State Change 3-133
19407 - Failed to Send Transport DATA Message 3-134
19408 - Single Transport Egress-Queue Utilization 3-135
19409 - Message Rejected by ACL Filtering 3-136
19410 - Adjacent Node IP Address State Change 3-136
19411 - SCTP Transport Closed Due to Failure of Multi-Homing Validation 3-137
19412 - SCTP Transport Configuration Mismatched for Adjacent Node IP 3-138
19413 - SCTP Transport Closed Due to Unsupported Peer Address Event Received 3-138
Communication Agent, ComAgent (19420-19909) 3-139
19420 - BDFQFull - Broadcast Data Framework Work Queue Full 3-139
19421 - BDFThrotl - Broadcast Data Framework Throttle Traffic 3-140
19422 - BDFInvalidPkt - Broadcast Data Framework Invalid Corrupt StackEvent 3-140
19800 - Communication Agent Connection Down 3-141
19801 - Communication Agent Connection Locally Blocked 3-142
19802 - Communication Agent Connection Remotely Blocked 3-143
19803 - Communication Agent Stack Event Queue Utilization 3-145
19804 - Communication Agent configured connection waiting for remote client to establish connection 3-146
19805 - Communication Agent Failed To Align Connection 3-148
19806 - Communication Agent CommMessage Mempool Utilization 3-149
19807 - Communication Agent User Data FIFO Queue Utilization 3-150
19808 - Communication Agent Connection FIFO Queue utilization 3-151
19810 - Communication Agent Egress Message Discarded 3-152
19811 - Communication Agent Ingress Message Discarded 3-153
19814 - Communication Agent Peer has not responded to heartbeat 3-154
19816 - Communication Agent Connection State Changed 3-154
19817 - Communication Agent DB Responder detected a change in configurable control option parameter 3-155
19818 - Communication Agent DataEvent Mempool utilization 3-156
19820 - Communication Agent Routed Service Unavailable 3-156
19821 - Communication Agent Routed Service Degraded 3-157
19822 - Communication Agent Routed Service Congested 3-158
19823 - Communication Agent Routed Service Using Low-Priority Connection Group 3-159

19824 - Communication Agent Pending Transaction Utilization 3-160
19825 - Communication Agent Transaction Failure Rate 3-162
19826 - Communication Agent Connection Congested 3-163
19827 - SMS stack event queue utilization 3-164
19830 - Communication Agent Service Registration State Change 3-165
19831 - Communication Agent Service Operational State Changed 3-165
19832 - Communication Agent Reliable Transaction Failed 3-166
19833 - Communication Agent Service Egress Message Discarded 3-167
19842 - Communication Agent Resource-Provider Registered 3-167
19843 - Communication Agent Resource-Provider Resource State Changed 3-168
19844 - Communication Agent Resource-Provider Stale Status Received 3-168
19845 - Communication Agent Resource-Provider Deregistered 3-169
19846 - Communication Agent Resource Degraded 3-169
19847 - Communication Agent Resource Unavailable 3-170
19848 - Communication Agent Resource Error 3-171
19850 - Communication Agent Resource-User Registered 3-171
19851 - Communication Agent Resource-User Deregistered 3-172
19852 - Communication Agent Resource Routing State Changed 3-172
19853 - Communication Agent Resource Egress Message Discarded 3-173
19854 - Communication Agent Resource-Provider Tracking Table Audit Results 3-174
19855 - Communication Agent Resource Has Multiple Actives 3-174
19856 - Communication Agent Service Provider Registration State Changed 3-175
19857 - Communication Agent Service Provider Operational State Changed 3-175
19858 - Communication Agent Connection Rejected 3-176
19860 - Communication Agent Configuration Daemon Table Monitoring Failure 3-176
19861 - Communication Agent Configuration Daemon Script Failure 3-178
19862 - Communication Agent Ingress Stack Event Rate 3-179
19863 - Communication Agent Max Connections Limit In Connection Group Reached 3-179
19864 - ComAgent Successfully Set Host Server Hardware Profile 3-180
19865 - ComAgent Failed to Set Host Server Hardware Profile 3-180
19866 - Communication Agent Peer Group Status Changed 3-181
19867 - Communication Agent Peer Group Egress Message Discarded 3-181
19868 - Communication Agent Connection Rejected - Incompatible Network 3-182
19900 - Process CPU Utilization 3-183
19901 - CFG-DB Validation Error 3-184
19902 - CFG-DB Update Failure 3-184
19903 - CFG-DB post-update Error 3-185
19904 - CFG-DB Post-Update Failure 3-186
19905 - Measurement Initialization Failure 3-187
Diameter Signaling Router (DSR) Diagnostics (19910-19999) 3-188

19910 - Message Discarded at Test Connection 3-188
19911 - Test message discarded 3-188
Diameter Alarms and Events (8000-8299, 22000-22350, 22900-22999, 25600-25899) 3-189
8000 - MpEvFsmException 3-189
8000 - 001 - MpEvFsmException_SocketFailure 3-189
8000 - 002 - MpEvFsmException_BindFailure 3-190
8000 - 003 - MpEvFsmException_OptionFailure 3-190
8000 - 004 - MpEvFsmException_AcceptorCongested 3-191
8000 - 101 - MpEvFsmException_ListenFailure 3-191
8000 - 102 - MpEvFsmException_PeerDisconnected 3-192
8000 - 103 - MpEvFsmException_PeerUnreachable 3-192
8000 - 104 - MpEvFsmException_CexFailure 3-193
8000 - 105 - MpEvFsmException_CerTimeout 3-194
8000 - 106 - MpEvFsmException_AuthenticationFailure 3-194
8000 - 201 - MpEvFsmException_UdpSocketLimit 3-195
8001 - MpEvException 3-195
8001 - 001 - MpEvException_Oversubscribed 3-195
8002 - MpEvRxException 3-196
8002 - 001 - MpEvRxException_DiamMsgPoolCongested 3-196
8002 - 002 - MpEvRxException_MaxMpsExceeded 3-196
8002 - 003 - MpEvRxException_CpuCongested 3-197
8002 - 004 - MpEvRxException_SigEvPoolCongested 3-198
8002 - 005 - MpEvRxException_DstMpUnknown 3-198
8002 - 006 - MpEvRxException_DstMpCongested 3-199
8002 - 007 - MpEvRxException_DrlReqQueueCongested 3-199
8002 - 008 - MpEvRxException_DrlAnsQueueCongested 3-200
8002 - 009 - MpEvRxException_ComAgentCongested 3-200
8002 - 201 - MpEvRxException_MsgMalformed 3-201
8002 - 202 - MpEvRxException_PeerUnknown 3-201
8002 - 203 - MpEvRxException_RadiusMsgPoolCongested 3-202
8002 - 204 - MpEvRxException_ItrPoolCongested 3-203
8002 - 205 - MpEvRxException_RclRxTaskQueueCongested 3-203
8002 - 206 - MpEvRxException_RclSigEvPoolCongested 3-204
8002 - 207 - MpEvRxException_ReqDuplicate 3-205
8002 - 208 - MpEvRxException_SharedSecretUnavailable 3-206
8003 - MpEvTxException 3-206
8003 - 001 - MpEvTxException_ConnUnknown 3-206
8003 - 101 - MpEvTxException_DclTxTaskQueueCongested 3-207
8003 - 201 - MpEvTxException_RclTxTaskQueueCongested 3-207
8003 - 202 - MpEvTxException_EtrPoolCongested 3-208

8003 - 203 - MpEvTxException_RadiusMsgPoolCongested 3-209
8003 - 204 - MpEvTxException_RadiusIdPoolCongested 3-209
8003 - 205 - MpEvTxException_SharedSecretUnavailable 3-210
8004 - EvFsmAdState 3-211
8004 - 001 - EvFsmAdState_StateChange 3-211
8005 - EvFsmOpState 3-211
8005 - 001 - EvFsmOpState_StateChange 3-211
8006 - EvFsmException 3-212
8006 - 001 - EvFsmException_DnsFailure 3-212
8006 - 002 - EvFsmException_ConnReleased 3-213
8006 - 101 - EvFsmException_SocketFailure 3-213
8006 - 102 - EvFsmException_BindFailure 3-214
8006 - 103 - EvFsmException_OptionFailure 3-215
8006 - 104 - EvFsmException_ConnectFailure 3-215
8006 - 105 - EvFsmException_PeerDisconnected 3-216
8006 - 106 - EvFsmException_PeerUnreachable 3-216
8006 - 107 - EvFsmException_CexFailure 3-217
8006 - 108 - EvFsmException_CeaTimeout 3-217
8006 - 109 - EvFsmException_DwaTimeout 3-218
8006 - 110 - EvFsmException_DwaTimeout 3-218
8006 - 111 - EvFsmException_ProvingFailure 3-219
8006 - 112 - EvFsmException_WatchdogFailure 3-219
8006 - 113 - EvFsmException_AuthenticationFailure 3-220
8007 - EvException 3-221
8007 - 101 - EvException_MsgPriorityFailure 3-221
8008 - EvRxException 3-221
8008 - 001 - EvRxException_MaxMpsExceeded 3-221
8008 - 101 - EvRxException_MsgMalformed 3-222
8008 - 102 - EvRxException_MsgInvalid 3-222
8008 - 201 - EvRxException_SharedSecretUnavailable 3-223
8008 - 202 - EvRxException_MsgAttrLenUnsupported 3-223
8008 - 203 - EvRxException_MsgTypeUnsupported 3-224
8008 - 204 - EvRxException_AnsOrphaned 3-224
8008 - 205 - EvRxException_AccessAuthMissing 3-225
8008 - 206 - EvRxException_StatusAuthMissing 3-225
8008 - 207 - EvRxException_MsgAuthInvalid 3-226
8008 - 208 - EvRxException_ReqAuthInvalid 3-226
8008 - 209 - EvRxException_AnsAuthInvalid 3-227
8008 - 210 - EvRxException_MsgAttrAstUnsupported 3-227
8008 - 212 - EvRxException_MsgTypeMissingMccs 3-228
8008 - 213 - EvRxException_ConnUnavailable 3-228

8009 - EvTxException 3-229
8009 - 001 - EvTxException_ConnUnavailable 3-229
8009 - 101 - EvTxException_DclTxConnQueueCongested 3-229
8009 - 102 - EvTxException_DtlsMsgOversized 3-230
8009 - 201 - EvTxException_MsgAttrLenUnsupported 3-230
8009 - 202 - EvTxException_MsgTypeUnsupported 3-231
8009 - 203 - EvTxException_MsgLenInvalid 3-232
8009 - 204 - EvTxException_ReqOnServerConn 3-232
8009 - 205 - EvTxException_AnsOnClientConn 3-233
8009 - 206 - EvTxException_DiamMsgMisrouted 3-233
8009 - 207 - EvTxException_ReqDuplicate 3-234
8009 - 208 - EvTxException_WriteFailure 3-234
8010 - MpIngressDrop 3-235
8011 - EcRate 3-236
8012 - MpRxNgnPsOfferedRate 3-237
8013 - MpNgnPsStateMismatch 3-238
8014 - MpNgnPsDrop 3-238
8015 - NgnPsMsgMisrouted 3-239
8016 - MpP16StateMismatch 3-240
8017 - MpTaskCpuCongested 3-241
8018 - P16MsgMisrouted 3-241
8019 - MpAnswerPriorityModeMismatch 3-242
8020 - MpRoutingThreadPoolStateMismatch 3-243
8100 - NormMsgMisrouted 3-243
8101 - DiagMsgMisrouted 3-244
8200 - MpRadiusMsgPoolCongested 3-244
8201 - RclRxTaskQueueCongested 3-245
8202 - RclItrPoolCongested 3-245
8203 - RclTxTaskQueueCongested 3-246
8204 - RclEtrPoolCongested 3-247
8205 - RadiusXactionFail 3-248
8206 - MpRxRadiusAllLen 3-248
8207 - MpRadiusKeyError 3-249
22001 - Message Decoding Failure 3-249
22002 - Peer Routing Rules with Same Priority 3-250
22003 - Application ID Mismatch with Peer 3-251
22004 - Maximum pending transactions allowed exceeded 3-251
22005 - No peer routing rule found 3-252
22007 - Inconsistent Application ID Lists from a Peer 3-253
22008 - Orphan Answer Response Received 3-254
22009 - Application Routing Rules with Same Priority 3-255

22010 - Specified DAS Route List not provisioned 3-255
22012 - Specified MCCS not provisioned 3-256
22013 - DAS Peer Number of Retransmits Exceeded for Copy 3-256
22014 - No DAS Route List specified 3-257
22016 - Peer Node Alarm Aggregation Threshold 3-258
22017 - Route List Alarm Aggregation Threshold 3-259
22018 - Maintenance Leader HA Notification to go Active 3-260
22019 - Maintenance Leader HA Notification to go OOS 3-260
22020 - Copy Message size exceeded the system configured size limit 3-261
22021 - Debug Routing Info AVP Enabled 3-261
22022 - Forwarding Loop Detected 3-262
22051 - Peer Unavailable 3-263
22052 - Peer Degraded 3-264
22053 - Route List Unavailable 3-265
22054 - Route List Degraded 3-266
22055 - Non-Preferred Route Group in Use 3-267
22056 - Connection Admin State Inconsistency Exists 3-268
22057 - ETG Rate Limit Degraded 3-269
22058 - ETG Pending Transaction Limit Degraded 3-270
22059 - Egress Throttle Group Message Rate Congestion Level changed 3-271
22060 - Egress Throttle Group Pending Transaction Limit Congestion Level changed 3-272
22061 - Egress Throttle Group Monitoring stopped 3-272
22062 - Actual Host Name cannot be determined for Topology Hiding 3-273
22063 - Diameter Max Message Size Limit Exceeded 3-274
22064 - Upon receiving Redirect Host Notification the Request has not been submitted for re-routing 3-274
22065 - Upon receiving Redirect Realm Notification the Request has not been submitted for re-routing 3-275
22066 - ETG-ETL Scope Inconsistency 3-275
22067 - ETL-ETG Invalid Association 3-276
22068 - TtpEvDoicException 3-277
- 22068 - 001 - TtpEvDoicException: DOIC OC-Supported-Features AVP not received 3-277
- 22068 - 002 - TtpEvDoicException: DOIC OC-Feature-Vector AVP contains an invalid value 3-277
- 22068 - 003 - TtpEvDoicException: DOIC OC-Report-Type AVP contains an unsupported value 3-278
- 22068 - 004 - TtpEvDoicException: DOIC OC-Sequence-Number AVP contains an out of order sequence number 3-278
- 22068 - 005 - TtpEvDoicException: DOIC OC-Reduction-Percentage AVP contains an invalid value 3-279

22068 - 006 - TtpEvDoicException: DOIC OC-Validity-Duration AVP contains an invalid value 3-280
22069 - TtpEvDoicOlr 3-280
22069 - 001 - TtpEvDoicOlr: Valid DOIC OLR Applied to TTP 3-280
22070 - TtpEvDegraded 3-281
22070 - 001 - TtpEvDegraded: TTP Degraded, Peer Overload 3-281
22070 - 002 - TtpEvDegraded: TTP Degraded, Peer Overload Recovery 3-281
22070 - 003 - TtpEvDegraded: TTP Degraded, Static Rate Limit Exceeded 3-282
22071 - TtgEvLossChg 3-282
22071 - 001 - TtgEvLossChg: TTG Loss Percent Changed 3-282
22072 - TTP Degraded 3-283
22073 - TTP Throttling Stopped 3-283
22074 - TTP Maximum Loss Percentage Threshold Exceeded 3-284
22075 - Message is not routed to Application 3-284
22076 - TTG Maximum Loss Percentage Threshold Exceeded 3-285
22077 - Excessive Request Reroute Threshold Exceeded 3-286
22078 - Loop or Maximum Depth Exceeded in ART or PRT Search 3-287
22082 - RouteList is not Provisioned in System Options 3-287
22101 - Connection Unavailable 3-288
22102 - Connection Degraded 3-289
22103 - SCTP Connection Impaired 3-292
22104 - SCTP Peer is Operating with a Reduced IP Address Set 3-293
22105 - Connection Transmit Congestion 3-294
22106 - Ingress Message Discarded: DraWorker Ingress MessageRate Control 3-295
22200 - MP CPU Congested 3-296
22201 - MpRxAllRate 3-297
22202 - MpDiamMsgPoolCongested 3-298
22203 - PTR Buffer Pool Utilization 3-299
22204 - Request Message Queue Utilization 3-299
22205 - Answer Message Queue Utilization 3-300
22206 - Reroute Queue Utilization 3-301
22207 - DclTxTaskQueueCongested 3-302
22208 - DclTxConnQueueCongested 3-302
22209 - Message Copy Disabled 3-303
22214 - Message Copy Queue Utilization 3-303
22221 - Routing MPS Rate 3-304
22222 - Long Timeout PTR Buffer Pool Utilization 3-305
22223 - DraWorker Memory Utilization Threshold Crossed 3-305
22224 - Average Hold Time Limit Exceeded 3-307
22225 - Average Message Size Limit Exceeded 3-309
22328 - Connection is processing a higher than normal ingress messaging rate 3-311

22349 - IPFE Connection Alarm Aggregation Threshold 3-312
22350 - Fixed Connection Alarm Aggregation Threshold 3-314
22900 - DPI DB Table Monitoring Overrun 3-316
22901 - DPI DB Table Monitoring Error 3-316
22950 - Connection Status Inconsistency Exists 3-317
22960 - DA-MP Profile Not Assigned 3-318
22961 - Insufficient Memory for Feature Set 3-318
25607 - DSR Signaling Firewall is administratively Disabled 3-319
25608 - Abnormal DA-MP Firewall 3-320
25609 - Firewall Configuration Error encountered 3-320
25610 - DSR Signaling Firewall configuration inconsistency detected 3-321
25611 - ETG - Invalid DRMP Attributes 3-321
25612 - Peer CNDRA ping failed 3-322
25613 – Peer Node Alarm Group Threshold 3-323
25614 - Connection Alarm Group Threshold 3-323
25805 - Invalid Shared TTG Reference 3-324
25806 - Invalid Internal Overseer Server Group Designation 3-325
Range Based Address Resolution (RBAR) Alarms and Events (22400-22424) 3-325
22400 - Message Decoding Failure 3-325
22401 - Unknown Application ID 3-326
22402 - Unknown Command Code 3-326
22403 - No Routing Entity Address AVPs 3-327
22404 - No valid Routing Entity Addresses found 3-328
22405 - Valid address received didn’t match a provisioned address or address range 3-328
22406 - Routing attempt failed due to internal resource exhaustion 3-329
22407 - Routing attempt failed due to internal database inconsistency failure 3-329
22411 - Address Range Lookup for Local Identifier skipped 3-330
Generic Application Alarms and Events (22500-22599) 3-331
22500 - Peer CNDRA Application Unavailable 3-331
22501 - Peer CNDRA Application Degraded 3-332
22502 - Peer CNDRA Application Request Message Queue Utilization 3-334
22503 - Peer CNDRA Application Answer Message Queue Utilization 3-335
22504 - Peer CNDRA Application Ingress Message Rate 3-336
22520 - Peer CNDRA Application Enabled 3-337
22521 - Peer CNDRA Application Disabled 3-338
Full Address Based Resolution (FABR) Alarms and Events (22600-22640) 3-338
22600 - Message Decoding Failure 3-338
22601 - Unknown Application ID 3-339
22602 - Unknown Command Code 3-340
22603 - No Routing Entity Address AVPs 3-340

22604 - No Valid User Identity Addresses Found 3-341
22605 - No Destination address is found to match the valid User Identity address 3-342
22606 - Database or DB connection error 3-343
22607 - Routing attempt failed due to DRL queue exhaustion 3-343
22608 - Database query could not be sent due to DB congestion 3-344
22609 - Database connection exhausted 3-344
22610 - FABR DP Service congestion state change 3-345
22611 - FABR Blacklisted Subscriber 3-345
22631 - FABR DP Response Task Message Queue Utilization 3-346
22632 - ComAgent Registration Failure 3-346
Policy and Charging Application (PCA) Alarms and Events (22700-22799) 3-348
22700 - Protocol Error in Diameter Requests 3-348
22701 - Protocol Error in Diameter Answers 3-348
22702 - Database Hash Function Error 3-349
22703 - Diameter Message Routing Failure Due To Full DRL Queue 3-350
22704 - Communication Agent Error 3-350
22705 - SBR Error Response Received 3-351
22706 - Binding Key Not Found In Diameter Message 3-351
22707 - Diameter Message Processing Failure 3-352
22708 - PCA Function is Disabled 3-353
22709 - PCA Function is Unavailable 3-353
22710 - SBR Sessions Threshold Exceeded 3-354
22711 - SBR Database Error 3-355
22712 - SBR Communication Error 3-356
22713 - SBR Alternate Key Creation Error 3-356
22714 - SBR RAR Initiation Error 3-357
22715 - SBR Audit Suspended 3-357
22716 - SBR Audit Statistics Report 3-358
22717 - SBR Alternate Key Creation Failure Rate 3-359
22718 - Binding Not Found for Binding Dependent Session Initiate Request 3-359
22719 - Maximum Number of Sessions per Binding Exceeded 3-360
22720 - Policy SBR To PCA Response Queue Utilization Threshold Exceeded 3-360
22721 - Policy and Charging Server In Congestion 3-361
22722 - Policy Binding Sub-resource Unavailable 3-362
22723 - Policy and Charging Session Sub-resource Unavailable 3-363
22724 - Policy SBR Memory Utilization Threshold Exceeded 3-365
22725 - SBR Server In Congestion 3-365
22726 - SBR Queue Utilization Threshold Exceeded 3-366
22727 - SBR Initialization Failure 3-367
22728 - SBR Bindings Threshold Exceeded 3-368

22729 - PCRF Not Configured 3-369
22730 - Policy and Charging Configuration Error 3-370
22731 - Policy and Charging Database Inconsistency 3-371
22732 - SBR Process CPU Utilization Threshold Exceeded 3-372
22733 - SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration 3-373
22734 - Policy and Charging Unexpected Stack Event Version 3-373
22735 - Policy DRA session initiation request received with no APN 3-374
22736 - SBR failed to free shared memory after a PCA function is disabled 3-375
22737 - Configuration Database Not Synced 3-376
22738 - SBR Database Reconfiguration State Transition 3-376
22740 - SBR Reconfiguration Plan Completion Failure 3-377
22741 - Failed to route PCA generated RAR 3-378
22742 - Enhanced Overload Control AdminState Mismatch 3-378
22743 - PCA Server Congested Due to Composite Resource Congestion 3-379
22750 - Enhanced Suspect Binding Removal Feature Enabled 3-380
22751 - Binding Audit Suppression by Suspect Binding Removal 3-380
22752 - SBR Process Not Running 3-381
SCEF (23000-23200, 102801-115001, 390000) 3-381
23150 - Diameter Application Not Supported 3-381
23152 - Universal SBR Sub-Resource Unavailable 3-382
23153 - Diameter Command Code not supported 3-383
23154 - HTTP Message Processing Error 3-383
23155 - SCEF Configuration Error 3-384
23156 - Protocol Error in Diameter Message 3-384
23157 - Protocol Error in HTTP Message 3-385
23158 - Universal SBR Error 3-385
23159 - Diameter Request Routing Failure 3-386
23160 - Access Control Not Enabled 3-386
23161 - USBR Response Queue Utilization Threshold Exceeded 3-387
23162 - Polling Event Queue Utilization Threshold Exceeded 3-387
102801 - 3-388
102826 - 3-388
102827 - 3-389
102828 - 3-389
102829 - 3-390
102830 - 3-390
102831 - 3-391
102832 - 3-391
102833 - 3-392
102834 - 3-392

102835 - 3-393
102836 - 3-393
102837 - 3-394
102838 - 3-394
102839 - 3-395
102840 - 3-395
102844 - 3-396
102845 - 3-396
102846 - 3-397
111007 - 3-397
115001 - 3-398
390000 - 3-398
Tekelec Virtual Operating Environment, TVOE (24400-24499) 3-399
24400 - TVOE libvirtd is down 3-399
24401 - TVOE libvirtd is hung 3-399
24402 - all TVOE libvirtd connections are in use 3-400
Computer Aided Policy Making, CAPM (25000-25499) 3-400
25000 - CAPM Update Failed 3-400
25001 - CAPM Action Failed 3-401
25002 - CAPM Exit Rule Template 3-402
25003 - CAPM Exit Trigger 3-402
25004 - Script failed to load 3-403
25005 - CAPM Generic Event 3-403
25006 - CAPM Generic Alarm - Minor 3-404
25007 - CAPM Generic Alarm - Major 3-404
25008 - CAPM Generic Alarm - Critical 3-405
OAM Alarm Management (25500-25899) 3-405
25500 - No DA-MP Leader Detected Alarm 3-405
25510 - Multiple DA-MP Leader Detected Alarm 3-407
25800 - Peer Discovery Failure 3-408
25801 - Peer Discovery Configuration Error Encountered 3-408
25802 - Realm Expiration Approaching 3-409
25803 - Peer Discovery - Inconsistent Remote Host Port Assignment 3-410
25804 - Peer Discovery State Change 3-410
Platform (31000-32800) 3-411
31000 - S/W fault 3-411
31001 - S/W status 3-411
31002 - Process watchdog failure 3-412
31003 - Thread watchdog failure 3-412
31100 - Database replication fault 3-413
31101 - Database replication to slave failure 3-414

31102 - Database replication from master failure 3-415
31103 - DB replication update fault 3-416
31104 - DB replication latency over threshold 3-417
31105 - Database merge fault 3-417
31106 - Database merge to parent failure 3-418
31107 - Database merge from child failure 3-419
31108 - Database merge latency over threshold 3-420
31109 - Topology config error 3-420
31110 - Database audit fault 3-421
31111 - Database merge audit in progress 3-421
31112 - DB replication update log transfer timed out 3-422
31113 - DB replication manually disabled 3-422
31114 - DB replication over SOAP has failed 3-423
31115 - Database service fault 3-424
31116 - Excessive shared memory 3-424
31117 - Low disk free 3-425
31118 - Database disk store fault 3-425
31119 - Database updatelog overrun 3-426
31120 - Database updatelog write fault 3-426
31121 - Low disk free early warning 3-427
31122 - Excessive shared memory early warning 3-427
31123 - Database replication audit command complete 3-428
31124 - ADIC error 3-429
31125 - Database durability degraded 3-429
31126 - Audit blocked 3-430
31127 - DB replication audit complete 3-430
31128 - ADIC found error 3-431
31129 - ADIC found minor issue 3-431
31130 - Network health warning 3-432
31131 - DB ousted throttle behind 3-432
31132 - DB replication precedence relaxed 3-433
31133 - DB replication switchover exceeds threshold 3-433
31134 - DB site replication to slave failure 3-434
31135 - DB site replication from master failure 3-434
31136 - DB site replication precedence relaxed 3-435
31137 - DB site replication latency over threshold 3-436
31140 - Database perl fault 3-436
31145 - Database SQL fault 3-437
31146 - DB mastership fault 3-437
31147 - DB upsynclog overrun 3-438
31148 - DB lock error detected 3-438

31149 - DB late write nonactive 3-439
31150 - DB Health Impacted 3-440
31151 – DB Storage Persistent Failure 3-440
31200 - Process management fault 3-441
31201 - Process not running 3-441
31202 - Unkillable zombie process 3-442
31206 - Process mgmt monitoring fault 3-443
31207 - Process resource monitoring fault 3-443
31208 - IP port server fault 3-444
31209 - Hostname lookup failed 3-444
31213 - Process scheduler fault 3-445
31214 - Scheduled process fault 3-445
31215 - Process resources exceeded 3-446
31216 - SysMetric configuration error 3-447
31217 - Network health warning 3-447
31220 - HA configuration monitor fault 3-448
31221 - HA alarm monitor fault 3-448
31222 - HA not configured 3-449
31223 - HA heartbeat transmit failure 3-449
31224 - HA configuration error 3-450
31225 - HA service start failure 3-450
31226 - HA availability status degraded 3-451
31227 - HA availability status failed 3-452
31228 - HA standby offline 3-452
31229 - HA score changed 3-453
31230 - Recent alarm processing fault 3-454
31231 - Platform alarm agent fault 3-455
31232 - Late heartbeat warning 3-455
31233 - HA path down 3-456
31234 - Untrusted time upon initialization 3-456
31235 - Untrusted time after initialization 3-457
31236 - HA link down 3-458
31240 - Measurements collection fault 3-459
31250 - RE port mapping fault 3-459
31260 - SNMP agent 3-460
31261 - SNMP configuration error 3-460
31270 - Logging output 3-461
31280 - HA active to standby transition 3-461
31281 - HA standby to active transition 3-462
31282 - HA management fault 3-462
31283 - Lost communication with server 3-463

31284 - HA remote subscriber heartbeat warning 3-464
31285 - HA node join recovery entry 3-464
31286 - HA node join recovery plan 3-465
31287 - HA node join recovery complete 3-465
31288 - HA site configuration error 3-466
31290 - HA process status 3-466
31291 - HA election status 3-467
31292 - HA policy status 3-467
31293 - HA resource link status 3-468
31294 - HA resource status 3-468
31295 - HA action status 3-469
31296 - HA monitor status 3-469
31297 - HA resource agent info 3-470
31298 - HA resource agent detail 3-470
31299 - HA notification status 3-471
31300 - HA control status 3-471
31301 - HA topology events 3-472
31322 - HA configuration error 3-472
32100 - Breaker panel feed unavailable 3-473
32101 - Breaker panel breaker failure 3-473
32102 - Breaker panel monitoring failure 3-474
32103 - Power feed unavailable 3-475
32104 - Power supply 1 failure 3-475
32105 - Power supply 2 failure 3-476
32106 - Power supply 3 failure 3-476
32107 - Raid feed unavailable 3-477
32108 - Raid power 1 failure 3-477
32109 - Raid power 2 failure 3-478
32110 - Raid power 3 failure 3-478
32111 - Device failure 3-479
32112 - Device interface failure 3-479
32113 - Uncorrectable ECC memory error 3-481
32114 - SNMP get failure 3-482
32115 - TPD NTP daemon not synchronized failure 3-483
32116 - TPD server's time has gone backwards 3-484
32117 - TPD NTP offset check failure 3-486
32300 - Server fan failure 3-487
32301 - Server internal disk error 3-488
32302 - Server RAID disk error 3-489
32303 - Server Platform error 3-489
32304 - Server file system error 3-490

32305 - Server Platform process error 3-491
32306 - Server RAM shortage error 3-491
32307 - Server swap space shortage failure 3-492
32308 - Server provisioning network error 3-493
32309 - EAGLE network A error 3-494
32310 - EAGLE network B error 3-494
32311 - Sync network error 3-495
32312 - Server disk space shortage error 3-495
32313 - Server default route network error 3-496
32314 - Server temperature error 3-497
32315 - Server mainboard voltage error 3-498
32316 - Server power feed error 3-499
32317 - Server disk health test error 3-500
32318 - Server disk unavailable error 3-501
32319 - Device error 3-501
32320 - Device interface error 3-502
32321 - Correctable ECC memory error 3-503
32322 - Power supply A error 3-503
32323 - Power supply B error 3-504
32324 - Breaker panel feed error 3-505
32325 - Breaker panel breaker error 3-505
32326 - Breaker panel monitoring error 3-508
32327 - Server HA Keepalive error 3-510
32328 - DRBD is unavailable 3-510
32329 - DRBD is not replicating 3-511
32330 - DRBD peer problem 3-512
32331 - HP disk problem 3-512
32332 - HP smart array controller problem 3-513
32333 - HP hpacucliStatus utility problem 3-514
32334 - Multipath device access link problem 3-515
32335 - Switch link down error 3-515
32336 - Half open socket limit 3-516
32337 - Flash program failure 3-517
32338 - Serial mezzanine unseated 3-517
32339 - TPD max number of running processes error 3-518
32340 - TPD NTP daemon not synchronized error 3-518
32341 - TPD NTP daemon not synchronized error 3-520
32342 - NTP offset check error 3-521
32343 - TPD RAID disk 3-522
32344 - TPD RAID controller problem 3-522
32345 - Server upgrade snapshot(s) invalid 3-523

32346 - OEM hardware management service reports an error 3-524
32347 - The hwmgmtcliStatus daemon needs intervention 3-524
32348 - FIPS subsystem problem 3-525
32349 - File tampering 3-526
32350 - Security process terminated 3-526
32500 - Server disk space shortage warning 3-527
32501 - Server application process error 3-528
32502 - Server hardware configuration error 3-528
32503 - Server RAM shortage warning 3-529
32504 - Software configuration error 3-530
32505 - Server swap space shortage warning 3-530
32506 - Server default router not defined 3-531
32507 - Server temperature warning 3-532
32508 - Server core file detected 3-533
32509 - Server NTP daemon not synchronized 3-534
32510 - CMOS battery voltage low 3-535
32511 - Server disk self test warning 3-536
32512 - Device warning 3-536
32513 - Device interface warning 3-537
32514 - Server reboot watchdog initiated 3-537
32515 - Server HA failover inhibited 3-538
32516 - Server HA active to standby transition 3-539
32517 - Server HA standby to active transition 3-539
32518 - Platform health check failure 3-540
32519 - NTP offset check failure 3-540
32520 - NTP stratum check failure 3-541
32521 - SAS presence sensor missing 3-543
32522 - SAS drive missing 3-543
32523 - DRBD failover busy 3-544
32524 - HP disk resync 3-544
32525 - Telco fan warning 3-545
32526 - Telco temperature warning 3-546
32527 - Telco power supply warning 3-546
32528 - Invalid BIOS value 3-547
32529 - Server kernel dump file detected 3-548
32530 - TPD upgrade failed 3-548
32531 - Half open socket warning limit 3-549
32532 - Server upgrade pending accept/reject 3-549
32533 - TPD max number of running processes warning 3-550
32534 - TPD NTP source is bad warning 3-551
32535 - TPD RAID disk resync 3-552

32536 - TPD server upgrade snapshot(s) warning 3-552
32537 - FIPS subsystem warning event 3-553
32538 - Platform data collection error 3-554
32539 - Server patch pending accept/reject 3-554
32540 - CPU power limit mismatch 3-555
32700 - Telco switch notification 3-555
32701 - HIDS initialized 3-556
32702 - HIDS baseline deleted 3-556
32703 - HIDS enabled 3-556
32704 - HIDS disabled 3-557
32705 - HIDS monitoring suspended 3-557
32706 - HIDS monitoring resumed 3-557
32707 - HIDS baseline updated 3-558
Diameter Custom Applications (DCA) Framework Alarms and Events (33300-33630) 3-558
33300 - Create Application Version Failure 3-558
33301 - Update Config Data Failure 3-559
33302 - Delete Application Version Failure 3-559
33303 - UDR Event Queue Utilization 3-560
33304 - DCA Runtime Errors 3-560
33305 - DCA Procedure Not Found 3-561
33307 - Diameter Message Routing Failure Due To Full DRL Queue 3-562
33308 - DCA to UDR ComAgent Error 3-563
33309 - DCA Script Compilation Error 3-563
33311 - DCA Application Reloaded 3-564
33312 - DCA Script Generation Error 3-564
33315 - DCA Asynchronous Task Stops Processing 3-565
33316 - DCA AsyncTask Queue Utilization 3-565
33317 - DCA Fetch Log Error 3-566
33318 - DCA CreateAndSend Request Message Send Failed 3-566
DCA Custom MEAL Event Templates 3-567
33330-33429 - DcaCustomMeal.name + "Alrm" 3-567
33430-33630 - DcaCustomMeal.name + "Alrm" 3-567
Independent SBR Alarms and Events (12003-12010, 33730-33830) 3-568
12003 - SBR congestion state 3-568
12007 - SBR active sess binding threshold 3-568
12010 - SBR proc term 3-569
33730 - U-SBR database audit statistics report 3-570
vSTP Alarms and Events (70000-70060, 70100-70999) 3-571
70000 - Association Down 3-571
70001 - Link Down 3-571
70002 - RSP/Destination Unavailable 3-572

70003 - RSP/Destination Route Unavailable 3-573
70004 - Linkset Unavailable 3-573
70005 - Link Unavailable 3-574
70006 - Preferred Route Unavailable 3-574
70007 - Node Isolated - All Links Down 3-575
70008 - Linkset Restricted 3-576
70009 - Link Congested 3-576
70050 - SCTP Connection Refused 3-577
70051 - Failed to Configure Transport 3-578
70052 - Far-end Closed the Connection 3-578
70053 - SCTP Connection Closed 3-579
70054 - Remote IP Address State Change 3-579
70055 - Association Admin State Change 3-580
70056 - Link Admin State Change 3-580
70057 - Received Invalid M3UA Message 3-581
70058 - Received M3UA ERROR 3-582
70059 - Failed to Send DATA Message 3-583
70060 - TFP Received 3-584
70061 - TFA Received 3-584
70062 - TFR Received 3-584
70063 - TFC Received 3-585
70064 - MTP3 Routing Error 3-585
70065 - MTP3 Routing Error - Invalid NI 3-586
70066 - MTP3 Routing Error - Invalid SI 3-586
70067 - Failed to Receive DATA Message 3-587
70068 - vSTP EIR Application Status Changed 3-588
70069 - TCAP Invalid Parameter or Decode Failure 3-588
70070 - Message Encode Failed 3-589
70071 - Missing IMEI 3-589
70072 - Invalid IMEI Length 3-590
70073 - Unsupported TCAP Message Type 3-590
70075 - vSTP LSS Stack Event Queue Utilization 3-591
70076 - vSTP Logging Stack Event Queue Utilization 3-591
70077 - vSTP EIR Log Fetch Error 3-592
70078 - vSTP EIR Logging Error in MP 3-592
70079 - M3UA Ingress Message Discarded 3-593
70081 - vSTP M3RL Linkset Buffer Utilization 3-594
70082 - vSTP M3RL RSP Buffer Utilization 3-594
70083 - vSTP M2PA Retransmission Buffer Utilization 3-595
70084 - vSTP MTP2 Transmission and Retransmission Buffer Utilization 3-595
70091 - Missing Mandatory Parameter 3-596

70092 - Malformed Subscriber ID 3-597
70093 - Unexpected Value for Subscriber ID 3-597
70094 - Invalid MSISDN Length 3-597
70095 - ATINP Invalid Requested Info 3-598
70096 - Digits Truncated in Encoded Parameter 3-598
70100 - ATINP Application Status Changed 3-599
70101 - Transmission Association Queue Congestion Crossed 3-599
70102 - MTP3 Ingress Link MSU TPS Crossed 3-600
70103 - MTP3 Egress Link MSU TPS Crossed 3-601
70104 - MTP3 Ingress Link Management TPS Crossed 3-601
70105 - Transmission Association Queue Discard Crossed 3-602
70107 - vSTP SCCP Stack Event Queue Utilization 3-603
70108 - vSTP M3RL Stack Event Queue Utilization 3-603
70109 - vSTP M3RL Network Management Event Queue Utilization 3-604
70110 - vSTP M3UA Stack Event Queue Utilization 3-604
70111 - vSTP M2PA Stack Event Queue Utilization 3-605
70112 - vSTP M3UA Tx Stack Event Queue Utilization 3-605
70201 - M2PA link operational state changed 3-606
70202 - M2PA Link Failed 3-606
70203 - M2PA Ingress Message Discarded 3-607
70204 - M2PA Egress Message Discarded 3-607
70205 - M2PA Message Encoding Failed 3-608
70206 - M2PA Message Decoding Failed 3-608
70207 - M2PA Proving Period Timer Expired 3-609
70208 - M2PA Remote Congestion Timer(T6) Expired 3-609
70209 - Received Remote Processor Outage 3-610
70210 - Received Remote Out of Service 3-610
70220 - MTP2 Link admin state change 3-611
70221 - Failed to send message to TDM driver 3-611
70222 - Failed to receive message from TDM driver 3-612
70223 - MTP2 link operational state changed 3-612
70224 - MTP2 link failed 3-613
70225 - MTP2 Ingress message discarded 3-613
70226 - MTP2 Egress message discarded 3-614
70227 - Received Remote Out Of Service on MTP2 link 3-614
70251 - Subsystem Congested 3-615
70252 - Subsystem Prohibited 3-615
70210 - Received Remote Out of Service 3-616
70271 - SCCP Received Invalid Message 3-616
70272 - SCCP Message Translation Failed 3-617
70273 - SCCP Message Routing Failed 3-617

70274 - SGMG Message Invalid 3-618
70275 - GTT SCCP Loop Detected 3-618
70276 - GTT Load Sharing Failed 3-619
70277 – GTT Action Discard MSU 3-619
70278 – GTT Action Failed 3-620
70279 – GTT MBR Duplicate Set Type Failed 3-620
70280 – GTT MBR Duplicate Set Type Warning 3-621
70281 – GTT FLOBR Duplicate Set Name Failed 3-621
70282 - GTT FLOBR Duplicate Set Name Warning 3-622
70283 - GTT FLOBR Max Search Depth Failed 3-622
70284 - GTT FLOBR Max Search Depth Warning 3-623
70285 – MBR Decoding Failed 3-623
70286 - GTT Duplicate Action Processing Stopped 3-624
70291 - XUDT UDT Conversion Failed. 3-624
70292 - SCCP Encode Failure 3-625
70293 - SFAPP Decode Error 3-625
70294 - SFAPP Validation Matching State not found 3-626
70295 - SFAPP Validation Encoding Error 3-626
70296 - SFAPP Validation Response Timeout Error 3-627
70297 - SFAPP Validation Velocity Chk Failed. 3-627
70298 - SFAPP Validation Failed 3-628
70299 - SFAPP Invalid CC/NDC received 3-628
70300 - Updation failed in UDR 3-628
70301 - VSTP SFAPP Stack Event Queue Utilization 3-629
70302 - Invalid Length of Conditioned Digits 3-629
70303 - Conv to Intl Num - Dflt NC Not Found 3-630
70304 - MNP Circular Route Detected 3-630
70305 - Translation PC Type is ANSI 3-631
70306 - Invalid Digits in MAP MSISDN Parameter 3-631
70307 - Invalid Prefix/Suffix Digit Length 3-631
70308 - Translation PC is Local Point Code 3-632
70309 - ANSI Translation Not Supported 3-632
70310 - Too many digits for DRA parameter 3-633
70311 - IDPR CGPN encoding failed 3-633
70312 - IDPR CDPN encoding failed 3-634
70313 - IDPRCDPN(X) NPP SERVICE is OFF 3-634
70314 - IDPRCGPN NPP SERVICE is OFF 3-634
70315 - DESTINATION ADDRESS DECODING is FAIL 3-635
70316 - TCAP ENCODING is FAIL 3-635
70317 - OUT OF BOUND DIGIT 3-636
70318 - SMS MANDATORY PARAMETER MISSING 3-636

70319 - ADDRESS DECODING is FAIL 3-637
70320 - MNPCDPA MATCHES HOME SMSC 3-637
70331 - SCCP XUDT Reassembly Failure 3-638
70332 - SCCP XUDT Segmentation Failure 3-638
70351 – vSTP Maintenance Leader HA Notification to Go Active 3-638
70352 – vSTP Maintenance Leader HA notification to GO OOS 3-639
70353 – Routing DB Inconsistency Exists 3-639
70354 – vSTP DB Table Monitoring Overrun 3-640
70355 - vSTP DB Table Monitoring Error 3-640
70356 - Failed to Process Ingress MSU: Peer MP Unavailable or Congested 3-641
70371 - No vSTP-MP Leader Detected 3-641
70372 - Multiple vSTP-MP Leader Detected 3-642
70373 - Connection Alarm Aggregation Threshold Reached 3-642
70374 - Link Alarm Aggregation Threshold Reached 3-643
70375 - Linkset Alarm Aggregation Threshold Reached 3-643
70376 - Route Alarm Aggregation Threshold Reached 3-644
70377 - RSP Alarm Aggregation Threshold Reached 3-644
70378 - SLTC Failure 3-645
70379 - Unexpected TFA Received 3-645
70380 - Unexpected TFR Received 3-646
70381 - Unexpected TFP Received 3-646
70382 - Unexpected TFC Received 3-647
70383 - Invalid H0 H1 Code 3-648
70384 - TFC Generated 3-648
70385 - Change Over Order Performed 3-649
70386 - Emergency Change Over Performed 3-649
70387 - Changeback Timer Expired 3-649
70388 - UPU Received 3-650
70389 - Remote Blocked 3-650
70290 - RSP/Destination Restricted 3-651
70391 - RSP/Destination Route Restricted 3-652
70392 - MSU Failed MTP Screening 3-652
70411 - ANSI to ITU CDPA GT Conversion Failure 3-653
70401 - ANSI to ITU CGPA GT Conversion Failure 3-653
70402 - ITU to ANSI CDPA GT Conversion Failure 3-654
70403 - ITU to ANSI CGPA GT Conversion Failure 3-654
70404 - Affected PC Conversion Failure 3-655
70404 - OPC Conversion Failed 3-655
70406 - Conversion Failed. CGPA PC Alias Undefined 3-656
70407 - Conversion MSU Discard. SCCP MSU Too Large 3-656
70408 - Conversion MSU Discard. Invalid Segmentation Parameters 3-657

70409 - Conversion Failed. Incorrect SCCP Parameter Length 3-657
70410 - MTP3 Circular Loop Detected 3-658
70411 - Conversion MSU Discard. Invalid SCMG Message Type 3-658
70416 - SCCP Application MSU Discarded 3-659
70418 - Sccp Egress Tps Threshold Crossed 3-659
70420 - Unsupported ACN Object ID Length 3-660
70421 - Failed to Decode TCAP Parameters 3-660
70422 - INAP Called Party Number is Missing 3-660
70423 - Unexpected SI in TIF Stop Action 3-661
70424 - Modified MSU too large to route 3-661
70425 - ISUP IAM Decode Failed 3-662
70425 - ISUP IAM Decode Failed 3-662
70427 - ISUP Encode Failed 3-663
70428 - TIF CgPN NS Failure: CC mismatch in DN 3-663
70429 - VLR Status changed 3-664
70430 - Velocity Threshold Crossed 3-664
70431 - Dynamic VLR Profile Aging 3-664
70432 - Dynamic VLR Roaming Aging 3-665
70433 - Vstp Dynamic learning is turned OFF 3-665
70434 - Vstp Dynamic learning LEARN Mode Timer Expired 3-666
70435 - Vstp Dynamic learning Profile Table Full 3-666
70436 - Vstp Dynamic learning Roaming Table Full 3-667
70437 - VSTP Security Logging Stack Event Queue Utilization 3-667
70438 - Vstp Security Logging Error in MP 3-668
70439 - Vstp Security Log Fetch Error 3-668
70440 - Vstp Security Log Fetch Error at Remote Server 3-668
70446 - VstpServiceStackEventQueueUtil 3-669
70451 - serviceMpUnavailable 3-669
70458 - Transaction Not Found for Ack. 3-670
70454 - SMS Proxy SCCP Validation Failed 3-670
70448 - SMS Proxy Message Validation Response Timeout Error 3-671
70447 - Service Validation Failed 3-671
70450 - SMS Proxy Message Validation Encoding Error 3-672
70450 - Service Validation Decoding Error 3-672
70453 - SMS Proxy GT address blocked 3-672
70452 - SMS Proxy GT address allowed. 3-673
70456 - Serivce DOS Timer Timeout 3-673
70455 - Service MTFSM Invoke Timer Timeout. 3-674
Diameter Equipment Identity Register (EIR) (71000-71999) 3-674
71000 - EIR Message Decoding Failure 3-674
71001 - ECA Routing Attempt Failed 3-675

71002 - EIR Message Encoding Failure 3-675
71003 - EIR Application Unavailable 3-676
71004 - UDR DB Connection Error 3-676
71005 - EIR TPS Exceeded 3-677
71006 - EIR Logging Suspended 3-677
71007 - EIR Request Queue Utilization 3-678
71008 - EIR UDR Response Queue Utilization 3-678
71009 - EIR Application Congested 3-679
71010 - ComAgent Registration Failure 3-679
71011 - Fetch Log Failed at SO 3-680

4 Key Performance Indicators (KPIs)

General KPIs information 4-1
KPIs Overview 4-1
KPIs 4-1
KPIs Server Elements 4-1
Viewing KPIs 4-2
KPIs data export elements 4-2
Exporting KPIs 4-3
Computer Aided Policy Making (CAPM) KPIs 4-5
Communication Agent (ComAgent) KPIs 4-5
DCA Custom MEAL KPIs 4-5
DCA Framework KPIs 4-5
Diameter (DIAM) KPIs 4-6
DP KPIs 4-6
Equipment Identity Register (EIR) KPIs 4-7
IDIH KPIs 4-9
IP Front End (IPFE) KPIs 4-9
Message Processor (MP) KPIs 4-9
Full Address Based Resolution (FABR) KPIs 4-10
Platform KPIs 4-10
Policy and Charging Application (PCA) KPIs 4-11
Process-based KPIs 4-11
Provisioning KPIs 4-12
Range Based Address Resolution (RBAR) KPIs 4-13
SCEF KPIs 4-14
SS7/Sigtran KPIs 4-15
Subscriber Binding Repository (SBR) KPIs 4-15
U-SBR KPIs 4-16

List of Figures

2-1	Flow of Alarms	2-2
2-2	Alarm Indicators Legend	2-3
2-3	Trap Count Indicator Legend	2-3
3-1	Breaker Panel LEDs	3-506
3-2	Breaker Panel Setting	3-507

List of Tables

2-1	Alarm/Event ID Ranges	2-4
2-2	Alarm and Event Types	2-5
2-3	Active Alarms Elements	2-6
2-4	Schedule Active Alarm Data Export Elements	2-7
2-5	Graphical information components	2-11
2-6	Schedule Event Data Export Elements	2-13
2-7	Data Export Elements	2-17
2-8	Active Tasks Elements	2-20
2-9	Active Tasks Report Elements	2-23
2-10	Scheduled Tasks Elements	2-24
3-1	Parameter Table	3-160
3-2	Parameter Table	3-162
4-1	KPIs Server Elements	4-1
4-2	Schedule KPI Data Export Elements	4-3
4-3	CAPM KPIs	4-5
4-4	Communication Agent KPIs	4-5
4-5	DCA Custom MEAL KPIs	4-5
4-6	DCA Framework KPIs	4-6
4-7	DIAM KPIs	4-6
4-8	DP KPIs	4-6
4-9	Diameter EIR KPIs	4-7
4-10	SS7 EIR KPIs	4-8
4-11	IDIH KPIs	4-9
4-12	IPFE KPIs	4-9
4-13	MP KPIs	4-9
4-14	FABR KPIs	4-10
4-15	Platform KPIs	4-10
4-16	PCA KPIs	4-11
4-17	Process-based KPIs	4-11
4-18	Provisioning KPIs	4-12
4-19	RBAR KPIs	4-13
4-20	Non Arrayed KPIs	4-14
4-21	Arrayed KPIs	4-14
4-22	SS7/Sigtran KPIs	4-15
4-23	SBR KPIs	4-15

4-24 SBR-Binding KPIs 4-15
4-25 SBR-Session KPIs 4-16
4-26 U-SBR KPIs 4-16
4-27 vSTP KPIs 4-17

1 Introduction

This section contains an overview of the available information for DSR alarms and events. The contents include sections on the scope and audience of the documentation, as well as how to receive customer support assistance.

Revision History

Date	Description
July 2020	Added new vSTP Alarm - Alarm-ID 70437, 70438, 70439, 70440
August 2020	Added a new DCA Alarm: 33315.
September 2020	Removed the following sections: • DM-IWF (33000-33024) • MD-IWF (33050-33099) • GLA (33100-33149) • MD-IWF KPIs • DM-IWF KPIs • GLA KPIs • 33306 - U-SBR Resolution Failure • 33310 - U-SBR Sub-resource Unavailable • 33313 - DCA U-SBR Logical Name Mismatch • Updated the following sections: – 33303 - UDR Event Queue Utilization – 33305 - DCA Procedure Not Found – 33308 - DCA to UDR ComAgent Error – 33430-33630 - DcaCustomMeal.name + "Alrm"
November 2020	• Added a note about the KPI column name in the Exporting KPIs section. • Added descriptions of Disk and Shared memory to the following sections: – KPIs Overview – Table 4-1
May 2021	Added a new Event in the 22082 - RouteList is not Provisioned in System Options section as part of the Mobile Private Network vDRA (MPN vDRA) feature.

Overview

The *DSR Alarms and KPIs* documentation provides information about DSR alarms, events, and KPIs; and provides corrective maintenance procedures and other information used to maintain the system. This book contains the following:

- Information relevant to understanding alarms and events in the application
- Recovery procedures for addressing alarms and events, as necessary
- Procedures for viewing alarms and events, generating alarms reports, and viewing and exporting alarms and event history
- Information relevant to understanding KPIs in the application
- Procedure for viewing KPIs
- List of KPIs

Scope and Audience

This manual does not describe how to install or replace software or hardware.

This manual is intended for personnel who must maintain operation of the DSR. The manual lists alarms, events, and KPIs along with preventive and corrective procedures that help personnel maintain DSR.

The corrective maintenance procedures are those used in response to a system alarm or output message. These procedures are used to help detect, isolate, and repair faults.

Manual Organization

Information in this document is organized into the following sections:

- Introduction contains general information about this document, how to contact My Oracle Support.
- Alarms, Events, and KPIs Overview provides general information about the application's alarms, events, and KPIs.
- Alarms and Events provides information and recovery procedures for alarms and events, organized first by alarm category, and then numerically by the number that displays in the application.
- Key Performance Indicators (KPIs) provides detailed KPI information, organized alphabetically by KPI name.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access 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 My Oracle Support, 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.

2

Alarms, Events, and KPIs Overview

This section provides general information about the application's alarms, events, and KPIs.

Alarms Warning

> **Note:**
>
> For the most up-to-date information, refer to the MIB document posted with each software release on the Oracle Software Delivery Cloud (OSDC) site.

General alarms and events information

This section provides general information about alarms and events including an alarms overview, types of alarms/events, and alarms-related procedures.

Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the View History GUI menu option.

> **Note:**
>
> Alarms in this manual are shared with other applications and may not display in your specific application.

Alarms and Events Overview

Alarms provide information pertaining to a system's operational condition that a network manager may need to act upon. An alarm might represent a change in an external condition, for example, a communications link has changed from connected to disconnected state. Alarms can have these severities:

- Critical application error
- Major application error
- Minor application error
- Cleared

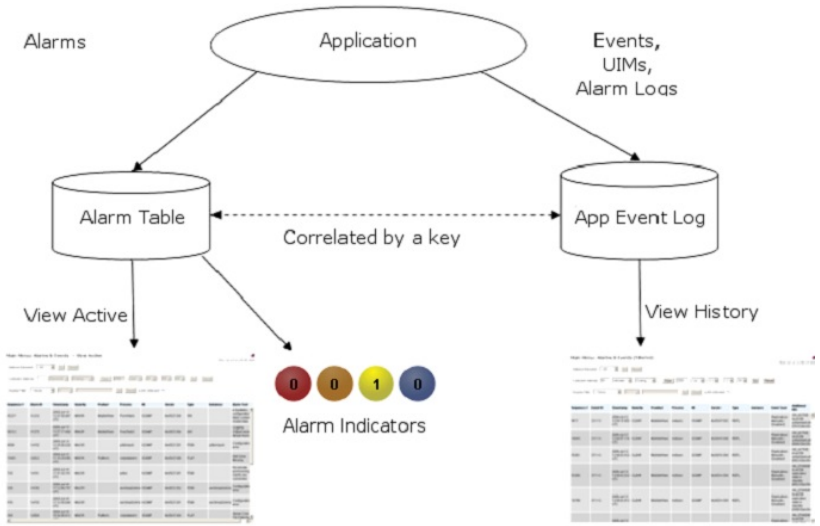
An alarm is considered inactive once it has been cleared and cleared alarms are logged on the **Alarms & Events**, and then **View History** page.

Events note the occurrence of an expected condition, such as an unsuccessful login attempt by a user. Events have a severity of Info and are logged on the View History page.

> **Note:**
>
> Some events may be throttled because the frequently generated events can overload the MP or OAM server's system or event history log (for example, generating an event for every ingress message failure). By specifying a throttle interval (in seconds), the events display no more than once during the interval duration period (for example, if the throttle interval is 5 seconds, the event is logged no more than once every 5 seconds).

Figure 2-1 shows how Alarms and Events are organized in the application.

Figure 2-1 Flow of Alarms



Alarms and events are recorded in a database log table. Application event logging provides an efficient way to record event instance information in a manageable form, and is used to:

- Record events representing alarmed conditions
- Record events for later browsing
- Implement an event interface for generating SNMP traps

Alarm indicators, located in the User Interface banner, indicate all critical, major, and minor active alarms. A number and an alarm indicator combined represent the number of active alarms at a specific level of severity. For example, if you see the number six in the orange-colored alarm indicator, it means there are six major active alarms. This is shown in Figure 2-2 and Figure 2-3.

Figure 2-2 Alarm Indicators Legend

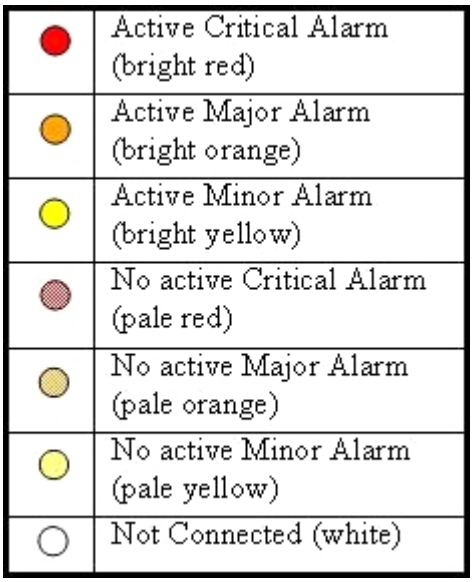
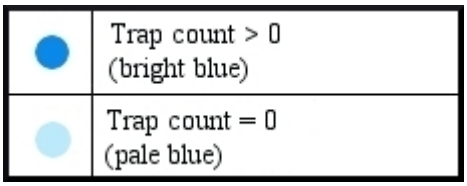


Figure 2-3 Trap Count Indicator Legend



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 Type: the type of alarm that has occurred. For a list of alarm types, see Alarm and Event Types.
- Description: describes the reason for the alarm
- Severity: the severity of the alarm
- Instance: the instance of a managed object for which an alarm or event is generated.

> **Note:**
>
> The value in the Instance field can vary, depending on the process generating the alarm.

- HA Score: high availability score; determines if switchover is necessary
- Auto Clear Seconds: the number of seconds that have to pass before the alarm will clear itself.

> **Note:**
>
> Some alarms and events have an Auto Clear Seconds of 0 (zero), indicating these alarms and events do not auto-clear

- OID: alarm identifier that appears in SNMP traps
- Recovery: provides any necessary steps for correcting or preventing the alarm

Alarm and Event ID Ranges

The **Alarm ID** listed for each alarm falls into one of the process classifications listed in Table 2-1.

Table 2-1 Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5999
OAM	10000-10999
IDIH	11500-11549
SDS	14000-14999
SS7/Sigtran	19200-19299
Transport Manager	19400-19419
Communication Agent (ComAgent)	19420-19909
DSR Diagnostics	19910-19999
Diameter	8000-8299, 22000-22350, 22900-2999, 25600-25899
Range Based Address Resolution (RBAR)	22400-22424
Generic Application	22500-22599
Full Address Based Resolution (FABR)	22600-22640
PDRA (aka PCA)	22700-22799
SCEF	23000-23200
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32800
Diameter Custom Applications (DCA)	33300-33630
Independent Subscriber Binding Repository (I-SBR)	33730-33830
vSTP	70000-70999
Equipment Identity Register (EIR)	71000-71999

Alarm and Event Types

Table 2-2 describes the possible alarm/event types that can be displayed.

> **Note:**
>
> Not all applications use all of the alarm types listed.

Table 2-2 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
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

Table 2-2 (Cont.) Alarm and Event Types

Type Name	Type
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

Active Alarms Elements

Active Alarms Elements describes the elements on the View Active alarms page.

Table 2-3 Active Alarms Elements

Active Alarms Element	Description
Sequence #	A system-wide unique number assigned to each alarm
Alarm ID	A unique number assigned to each alarm in the system. See Alarm and Event ID Ranges for more information.
Alarm Text	Description of the alarm. The description is truncated to 140 characters. **Note**: The **Alarm Text** field is not truncated in exports or reports.
Timestamp	Date and time the alarm occurred (fractional seconds resolution)
Severity	Alarm severity - Critical, Major, Minor
Product	Name of the product or application that generated the alarm
Process	Name of the process that generated the alarm
NE	Name of the Network Element where the alarm occurred
Server	Name of the server where the alarm occurred
Type	Alarm or Event Type, for example, Process, Disk, Platform. See Alarm and Event Types for more information.
Instance	Instance of the alarm, for example, Link01 or Disk02. The Instance provides additional information to help differentiate two or more alarms with the same number. This field may be blank if differentiation is not necessary

View Active Alarms

Active alarms are displayed in a scrollable, optionally filterable table. By default, the active alarms are sorted by time stamp with the most recent alarm at the top.

Use this procedure to view active alarms.

> **Note:**
>
> The alarms and events that appear in View Active vary depending on whether you are logged into an NOAM or SOAM. Alarm collection is handled solely by NOAM servers in systems that do not support SOAMs.

1. Click **Alarms & Events**, and then **View Active**.
2. If necessary, specify filter criteria and click **Go**.

   The active alarms are displayed according to the specified criteria.
   The active alarms table updates automatically. When new alarms are generated, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.

   The following message appears: `(Alarm updates are suspended.)`
   If a new alarm is generated while automatic updates are suspended, a new message appears: `(Alarm updates are suspended. Available updates pending.)`

   To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

Active Alarms Data Export Elements

Table 2-4 describes the elements on the **Alarms & Events**, and then **View Active**, and then **Export** form.

Table 2-4 Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Option Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly Default: Once **Note**: Depending on what upload frequency is selected, some scheduling choices may become inactive and the buttons or lists are grayed out. Note that the Fifteen Minute, Hourly, Daily, and Weekly scheduling options are only available when provisioning is enabled.

Table 2-4 (Cont.) Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task.	Format: Text box Range: Maximum length is 40 characters. Valid characters are alphanumeric, minus sign, and spaces between words. The first character must be an alpha character. The last character must not be a minus sign. Default: APDE Alarm Export. The default value can only be used once. For scheduled exports, the frequency is not Once, because the name must be unique. **Note**: This field is not active if the selected export frequency is once.
Description	Optional description of the scheduled task	Format: Text box Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character. **Note**: This field is not active if the selected export frequency is once.
Filename Prefix	Optional export filename prefix. The extension to pre-pend the generated export file name.	Format: Text box Range: Maximum length is 8 characters; alphanumeric (a-z, A-Z, and 0-9).
Minute	Select the minute of each hour when the data will be written to the export directory. Enabled only if Export Frequency is hourly or fifteen minutes. For a frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer in the hour, a value between 0 and 14.	Format: Scrolling list Range: 0 to 59 Default: 0 **Note**: This field is not active if the selected export frequency is Once, Daily, or Weekly. This field is only active if the selected export frequency is Fifteen Minutes or Hourly.
Time of Day	Select the time of day when the data will be written to the export directory. Enabled only if Export Frequency is daily or weekly. Select from 15-minute increments, or fill in a specific value.	Format: Time text box Range: HH:MM with AM/PM Default: 12:00 AM **Note**: This field is not active if the selected export frequency is Once, Fifteen Minutes, or Hourly. This field is only active if the selected export frequency is Daily or Weekly.

Table 2-4 (Cont.) Schedule Active Alarm Data Export Elements

Element	Description	Data Input Notes
Day of Week	Select the day of week when the data will be written to the export directory. Enabled only if Export Frequency is weekly.	Format: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday **Note**: This field is active only if Weekly is selected.

Export Active Alarms

You can initiate a one-time export task of active alarm data or schedule periodic exports from the **Alarms and Events**, and then **View Active** page. Active alarm data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the View Active page, only filtered data is exported.

For each export task, the system automatically creates a CSV file of the filtered data. The file is available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the remote server data export feature. For more information about using remote server data export, see Data Export.

Alarm details can be exported to a file by clicking **Export** on the View Active page. The system automatically creates and writes the exported active alarm details to a CSV file in the file management area.

Use this procedure to export active alarms to a file, or schedule a periodic data export task of this data.

1. Click **Alarms & Events**, and then **View Active**.
2. Locate and select the server group tab that contains the alarms of interest.

   Server groups are presented in tabular form. If the target server group is not visible in the available screen space, use the scroll right/left buttons located below the tool bar area and to the right or left of the visible tabs.
3. Click **Export**.
4. Select the **Export Frequency**. Based on this selection other fields may become active or inactive.
5. Type a **Task Name**.

   This field is not active if the selected export frequency is once. For more information about **Task Name**, or any field on this page, see Active Alarms Data Export Elements.
6. Optional: Type a **Description**.

   This field is not active if the selected export frequency is once.
7. Optional: Type a **Filename Prefix**.

   The filename prefix is prepended to the generated export file name for quick identification.
8. Select the **Minute** if **Export Frequency** is fifteen minutes or hourly.

If the selected export frequency is fifteen minutes or hourly, this is the minute of each period when the transfer is set to begin. For an export frequency of fifteen minutes, transfers occur four times per hour, and this field displays the minute of the first transfer of the hour.

9. Select the **Time of Day** if **Export Frequency** is daily or weekly.

   This field is not active if the selected export frequency is once, fifteen minutes, or hourly.

10. Select the **Day of Week** if **Export Frequency** is weekly.

    This field is not active if the selected export frequency is once, fifteen minutes, hourly, or daily.

11. Click **OK** to initiate the active alarms export task or **Cancel** to discard the changes and return to the View Active page.

The data export task is initiated or scheduled.
From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see View the File List.

Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**. For more information see:

- Editing a Scheduled Task
- Deleting a Scheduled Task
- Generating a Scheduled Task Report

> **Note:**
>
> Only one export operation at a time is supported on a single server. If an export is in progress from another GUI session when you click **Export**, a message is displayed and the export does not start. You must wait until the other export is complete before you can begin your export.

Generate a Report of Active Alarms

Use this procedure to generate a report.

1. Click **Alarms & Events**, and then **View Active**.
2. Specify filter criteria, if necessary, and click **Go**.

   The active alarms are displayed according to the specified criteria. Alternately, you can select multiple rows and generate a report using those. To select multiple rows, press and hold **Ctrl** as you click to select specific rows.

3. Click **Report**.

   The View Active Report can be printed or saved to a file.

4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Graph Active Alarms

The View Active alarm screen includes the ability to produce a set of summary graphs which provide statistical summaries of the active alarms. The active alarms can be graphed based on different topology characteristics or alarm data fields by selecting one or more components from the Graph list. The graphing selections are persistent.

The active alarm graphs display as a series of stacked bar graphs, one bar stack for each server. Each bar stack shows the count of critical, major and minor alarms for the selected items in the Graph list. Multiple graphs display side-by-side for each item selected. The graphs are displayed above the active alarms grid listing.

Use this procedure to graph active alarms:

1. Click **Alarms & Events**, and then **View Active**.
2. If necessary, specify filter criteria In the Filter list and click **Go**.

   The selected Filter criteria are applied to all Server Group tabs. The active alarms that meet the specified criteria display.
3. Specify one or more graphical information components from the Graph list. Valid components are listed in Table 2-5.

Table 2-5 Graphical information components

Topology Components	Alarm Data Field Components
Network Element	Event ID
Server	Severity
Server Group	Product
Resource Domain	Process
Place	Server
Place Association	Type

> **Note:**
>
> Server is both a topology component and a data field in the active alarm data grid display.

   The graphs for the selected components display above the tabbed area.
4. To adjust the graph viewing area, click and hold the slider above the graph while adjusting the proportions with the mouse.
5. To remove one or more graphs, de-select the choices from the **Graph** list.

   If only some choices are deselected, the deselected graphs disappear. If all choices are deselected, the graph display disappears.

Active Alarms Quick Filter

The individual information in the bar stacks of the active alarm graphs can be used to further filter the alarm information in the current Server Group tab. This allows a

more focused, quick look at the alarms. The quick filter selection(s) are not persistent. The quick filter settings are cleared once the user browses away from the View Active Alarms page.

Quick filter selections from the graph are applied to the grid and all graphs displayed within the current Server Group tab of the View Active Alarms page. For example, if the portion of the stacked bar graph that displays the critical alarms is selected, the grid filters to show critical platform alarms and the summary statistics are recalculated to adjust the graphs. If additional portions of the graphs are selected, both the grid and the graphs continue to be filtered according to the selections.

> **Note:**
>
> Although the quick filter is applied to the grid display, the quick filter criteria are not applied to generated Reports and Exports of active alarm data. Use the **Filter** list in the toolbar to filter the data.

Once active alarms have been graphed, use this procedure to apply a quick filter to active alarms in a server group:

1. To add a quick filter, select a portion of the stacked bar graph to filter. The stacked bar displays lists of active alarms by the alarm severity.

   > **Note:**
   >
   > Alarm severity types are displayed using the following color distinctions:
   >
   > - Critical - Red
   > - Major - Orange
   > - Minor - Yellow

   Upon selection, the filtered graph portion displays green to indicate it is being used as a filter.
2. Repeat the previous step as needed to filter additional portions of the remaining bar graphs.
3. To remove all quick filtering selections from the active Server Group tab, click **Clear Selections**.

   The display grid and all graphs display with no quick filtering.
4. To remove individual quick filtering selections from the active Server Group tab, select the portion of the stacked bar graph displayed in green.

   The display grid and all graphs recalculate based on the remaining selections.

Viewing alarm and event history

All historical alarms and events are displayed in a scrollable, optionally filterable table. The historical alarms and events are sorted, by default, by time stamp with the most recent one at the top. Use this procedure to view alarm and event history.

> **Note:**
>
> The alarms and events that appear in View History vary depending on whether you are logged in to an NOAM or SOAM. Alarm collection is handled solely by NOAM servers in systems that do not support SOAMs.

1. Click **Alarms & Events**, and then **View History**.
2. If necessary, specify filter criteria and click **Go**.

   > **Note:**
   >
   > Some fields, such as **Additional Info**, truncate data to a limited number of characters. When this happens, a **More** link displays. Click **More** to display a report with all relevant data.

   Historical alarms and events are displayed according to the specified criteria. The historical alarms table updates automatically. When new historical data is available, the table is automatically updated, and the view returns to the top row of the table.
3. To suspend automatic updates, click any row in the table.

   The following `(Alarm updates are suspended.)` message displays. If a new alarm is generated while automatic updates are suspended, the `(Alarm updates are suspended. Available updates pending.)` message displays.

   To resume automatic updates, press and hold **Ctrl** as you click to deselect the selected row.

Historical events data export elements

This table describes the elements on the **View History**, and then **Export** page.

Table 2-6 Schedule Event Data Export Elements

Element	Description	Data Input Notes
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.

Table 2-6 (Cont.) Schedule Event Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Options Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data is written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Options Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting alarm and event history

You can schedule periodic exports of historical data from the Alarms and Events View History page. Historical data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the View History page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the Export Server feature. For more information about using Export Server, see Data Export.

The details of historical alarms and events can be exported to a file by clicking the **Export** button on the View History page. The system automatically creates and writes the exported historical alarm details to a CSV file in the file management area.

If filtering has been applied in the View History page, only filtered historical alarms and events are exported. Use this procedure to export alarm and event history to a file. Use this procedure to schedule a data export task.

1. Select **Alarms & Events**, and then **View History**.
2. If necessary, specify filter criteria and click **Go**.

   The historical alarms and events are displayed according to the specified criteria.
3. Click **Export**.
4. Enter the **Task Name**.

   For more information about **Task Name**, or any field on this page, see Historical events data export elements.
5. Select the **Export Frequency**.

6. If you selected Hourly, specify the Minutes.
7. Select the **Time of Day**.

> **Note:**
>
> **Time of Day** is not an option if **Export Frequency** equals **Once**.

8. Select the **Day of Week**.

> **Note:**
>
> **Day of Week** is not an option if **Export Frequency** equals **Once**.

9. Click **OK** or **Apply** to initiate the data export task.

   The data export task is scheduled. From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see View the File List.

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage**, and then **Tasks**. For more information see:

   - Editing a Scheduled Task
   - Deleting a Scheduled Task
   - Generating a Scheduled Task Report

10. Click **Export**.
11. Click the link in the green message box to go directly to the **Status & Manage**, and then **Files** page.

   From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the alarm history file you exported during this procedure. For more information, see Opening a File.

Generating a report of historical alarms and events

Use this procedure to generate a report.

1. Click **Alarms & Events**, and then **View History**.
2. Specify filter criteria, if necessary, and click **Go**.

   The historical alarms and events are displayed according to the specified criteria.

3. Click **Report**.

   The View History Report can be printed or saved to a file.

4. Click **Print** to print the report.

5. Click **Save** to save the report to a file.

View the File List

Use this procedure to view the list of files located in the file management storage area of a server. The amount of storage space currently in use can also be viewed on the Files page.

1. From the Main menu, select **Status & Manage**, and then **Files**.
2. Select a server.

   All files stored on the selected server are displayed.

Opening a File

Use this procedure to open a file stored in the file management storage area.

1. Select **Status & Manage**, and then **Files**.
2. Select an **NE Name**.
3. Click **List Files**.

   The Status & Manage Files list page for the selected network element displays all files stored in its file management storage area.
4. Click the **Filename** of the file to be opened.
5. Click **Open** to open the file.

Data Export

From the Data Export page, you can set an export target to receive exported performance data. Several types of performance data can be filtered and exported using this feature. For more information about how to create data export tasks, see:

- Export Active Alarms
- Exporting alarm and event history
- Exporting KPIs

From the Data Export page, you can manage file compression strategy and schedule the frequency with which data files are exported.

Data Export elements

This table describes the elements on the **Administration**, and then **Remote Servers**, and then **Data Export** page.

Table 2-7 Data Export Elements

Element	Description	Data Input Notes
Hostname	Name of export server	Must be a valid hostname or a valid IP address. Range: Maximum length is 255 characters; alphanumeric characters (a-z, A-Z, and 0-9) and minus sign. Hostname must start and end with an alphanumeric. To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None
Username	Username used to access the export server	Format: Textbox Range: Maximum length is 32 characters; alphanumeric characters (a-z, A-Z, and 0-9). To clear the current export server and remove the file transfer task, specify an empty hostname and username. Default: None
Directory on Export Server	Directory path on the export server where the exported data files are to be transferred	Format: Textbox Range: Maximum length is 255 characters; valid value is any UNIX string. Default: None
Path to rsync on Export Server	Optional path to the rsync binary on the export server	Format: Textbox Range: Maximum length is 4096 characters; alphanumeric characters (a-z, A-Z, and 0-9),dash, underscore, period, and forward slash. Default: If no path is specified, the username's home directory on the export server is used
Backup File Copy Enabled	Enables or disables the transfer of the backup files	Format: Checkbox Default: Disabled (unchecked)
File Compression	Compression algorithm used when exported data files are initially created on the local host	Format: Option Range: gzip, bzip2, or none Default: gzip
Upload Frequency	Frequency at which the export occurs	Format: Option Range: fifteen minutes, hourly, daily or weekly Default: weekly

Table 2-7 (Cont.) Data Export Elements

Element	Description	Data Input Notes
Minute	If The Upload Frequency is Hourly, this is the minute of each hour when the transfer is set to begin	Format: Scrolling list Range: 0 to 59 Default: zero
Time of Day	If the Upload Frequency is Daily of Weekly, this is the time of day the export occurs	Format: Time textbox Range: HH:MM AM/PM in 15-minute increments Default: 12:00 AM
Day of Week	If Upload Frequency is Weekly, this is the day of the week when exported data files will be transferred to the export server.	Format: Option Range: Sunday through Saturday Default: Sunday
SSH Key Exchange	This button initiates an SSH key exchange between the OAM server and the data export server currently defined on the page. A password must be entered before the exchange can complete.	Format: Button
Transfer Now	This button initiates an immediate attempt to transfer any data files in the export directory to the export server.	Format: Button
Test Transfer	This button initiates an immediate test transfer to the data export server currently defined on the page.	Format: Button
Keys Report	This button generates an SSH Keys Report for all OAM servers.	Format: Button

Configuring data export

The Data Export page enables you to configure a server to receive exported performance and configuration data. Use this procedure to configure data export.

1. Select **Administration**, and then **Remote Servers**, and then **Data Export**.
2. Enter a **Hostname**.

   See Data Export elements for details about the **Hostname** field and other fields that display on this page.
3. Enter a **Username**.
4. Enter a **Directory Path** on the Export server.
5. (Optional) Enter the **Path to Rsync** on the Export server.

> **Note:**
>
> Depending on the OS and implementation of the remote server, it may be required to define the path to the rsync binary on the export server but this is not common. If no path is specified, the username's home directory on the export server is used.

6. Select whether to enable the transfer of the backup file. To leave the backup disabled, do not check the box.
7. Select the **File Compression** type.
8. Select the **Upload Frequency**.
9. If you selected hourly for the upload frequency, select the **Minute** intervals.
10. If you selected daily or weekly for the upload frequency, select the **Time of Day**.
11. If you selected weekly for the upload frequency, select the **Day of the Week**.
12. If public keys were manually placed on the Export server, skip to step 14.

    Otherwise, click **Exchange SSH Key** to transfer the SSH keys to the Export server.
13. Enter the password.

    The server attempts to exchange keys with the export server currently defined on the page. After the SSH keys are successfully exchanged, continue with the next step.
14. Click **OK** to apply the changes or **Cancel** to discard the changes.

    The export server is now configured and available to receive performance and configuration data.
15. You may optionally click **Test Transfer** to confirm the ability to export to the server currently defined on the page.

    The user can monitor the progress of the task by selecting the **Tasks** drop down list in the page control area.

Tasks

The Tasks pages display the active, long running tasks and scheduled tasks on a selected server. The Active Tasks page provides information such as status, start time, progress, and results for long running tasks, while the Scheduled Tasks page provides a location to view, edit, and delete tasks scheduled to occur.

Active Tasks

The Active Tasks page displays the long running tasks on a selected server. The Active Tasks page provides information such as status, start time, progress, and results, all of which can be generated into a report. Additionally, you can pause, restart, or delete tasks from this page.

Active Tasks elements

The Active Tasks page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. Table 2-8 describes elements on the Active Tasks page.

Table 2-8 Active Tasks Elements

Active Tasks Element	Description
ID	Task ID
Name	Task name
Status	Current status of the task. Status values include: running, paused, completed, exception, and trapped.
Start Time	Time and date when the task was started
Update Time	Time and date the task's status was last updated
Result	Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.
Result Details	Details about the result of the task
Progress	Current progress of the task

Deleting a task

Use this procedure to delete one or more tasks.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.
2. Select a server.

> **Note:**
>
> Hovering the cursor over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Select one or more tasks.

> **Note:**
>
> To delete a single task or multiple tasks, the status of each task selected must be one of the following: completed, exception, or trapped.

> **Note:**
>
> You can select multiple rows to delete at one time. To select multiple rows, press and hold Ctrl as you click to select specific rows.

4. Click **Delete**.
5. Click **OK** to delete the selected task(s).

Deleting all completed tasks

Use this procedure to delete all completed tasks.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.
2. Select a server.

> **Note:**
>
> Hovering the cursor over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Click **Delete all Completed**.
4. Click **OK** to delete all completed tasks.

Cancelling a running or paused task

Use this procedure to cancel a task that is running or paused.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.
2. Select a server.

> **Note:**
>
> Hovering the cursor over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Select a task.
4. Click **Cancel**.
5. Click **OK** to cancel the selected task.

Pausing a task

Use this procedure to pause a task.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.
2. Select a server.

> **Note:**
>
> Hovering the mouse over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Select a task.

> **Note:**
>
> A task may be paused only if the status of the task is running.

4. Click **Pause**.

   A confirmation box appears.

5. Click **OK** to pause the selected task.

   For information about restarting a paused task, see Restarting a task.

Restarting a task

Use this procedure to restart a task.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.
2. Select a server.

> **Note:**
>
> Hovering the mouse over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Select a paused task.

> **Note:**
>
> A task may be restarted only if the status of the task is paused.

4. Click **Restart**.

   A confirmation box appears.

5. Click **OK** to restart the selected task.

   The selected task is restarted.

Active Tasks report elements

The Active Tasks [Report] page displays report data for selected tasks. Table 2-9 describes elements on the Active Tasks [Report] page.

Table 2-9 Active Tasks Report Elements

Active Tasks Report Element	Description
Task ID	Task ID
Display Name	Task name
Task State	Current status of the task. Status values include: running, paused, completed, exception, and trapped.
Admin State	Confirms task status
Start Time	Time and date when the task was started
Last Update Time	Time and date the task's status was last updated
Elapsed Time	Time to complete the task
Result	Integer return code of the task. Values other than 0 (zero) indicate abnormal termination of the task. Each value has a task-specific meaning.
Result Details	Details about the result of the task

Generating an active task report

Use this procedure to generate an active task report.

1. Click **Status & Manage**, and then **Tasks**, and then **Active Tasks**.
2. Select a server.

> **Note:**
>
> Hovering the mouse over any tab displays the name of the server.

All active tasks on the selected server are displayed.

3. Select one or more tasks.

> **Note:**
>
> If no tasks are selected, all tasks matching the current filter criteria is included in the report.

4. Click **Report**.
5. Click **Print** to print the report.
6. Click **Save** to save the report.

Scheduled Tasks

The periodic export of certain data can be scheduled through the GUI. The Scheduled Tasks page provides you with a location to view, edit, delete, and generate reports

of these scheduled tasks. For more information about the types of data that can be exported, see:

- Export Active Alarms
- Exporting alarm and event history
- Exporting KPIs

Scheduled Tasks Elements

The Scheduled Tasks page displays information in a tabular format where each tab represents a unique server. By default, the current server's tab is selected when the page is loaded. Table 2-10 describes elements on the Scheduled Tasks page.

Table 2-10 Scheduled Tasks Elements

Scheduled Tasks Element	Description
Task Name	Name given at the time of task creation
Description	Description of the task
Time of Day	The hour and minute the task is scheduled to run
Day-of-Week	Day of the week the task is scheduled to run
Network Elem	The Network Element associated with the task

Editing a Scheduled Task

Use this procedure to edit a scheduled task.

1. Click **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.
2. Select a task.
3. Click **Edit**.
4. Edit the available fields as necessary.

   See Scheduled Tasks Elements for details about the fields that display on this page.
5. Click **OK** or **Apply** to submit the changes and return to the Scheduled Tasks page.

Deleting a Scheduled Task

Use this procedure to delete one or more scheduled tasks.

1. Click **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.
2. Select one or more tasks.
3. Click **Delete**.
4. Click **OK** to delete the selected task(s).

Generating a Scheduled Task Report

Use this procedure to generate a scheduled task report.

1. Click **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.

2. Select one or more tasks.

> **Note:**
>
> If no tasks are selected, all tasks matching the current filter criteria is included in the report.

3. Click **Report**.
4. Click **Print** to print the report.
5. Click **Save** to save the report.

3
Alarms and Events

This section provides general alarm/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. Currently active alarms can be viewed from **Alarms & Events**, and then **View Active**. The alarms and events log can be viewed from the View History option.

> **Note:**
>
> Some of the alarms in this document are shared with other applications and may not appear in this particular product.

IP Front End, IPFE (5000-5999)

This section provides information and recovery procedures for IP Front End (**IPFE**) alarms, which range from 5000 to 5999.

5001 - IPFE Backend Unavailable

Alarm Group:
IPFE

Description:
The IPFE has not received any heartbeats from an application server within the heartbeat timeout interval.

Severity:
Minor

Instance:
IP address of the application server.

> **Note:**
>
> If a heartbeat is received from the application server, this alarm clears.

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeBackendUnavailableNotify

Cause:
A DA-MP is not sending heartbeats to the IPFE.

Diagnostic Information:
Wireshark is the tool to monitor if the DAMP is sending a heartbeat to IPFE.
Follow these steps to diagnose the issues:

1. From the SO GUI, navigate to **IPFE**, and then **Configuration**, and then **Target Sets**, and then **TSA#**, and then **+**; and at least one DAMP server XSI IP should be present.

   If yes, go to step 2.

2. Log into the IPFE server.

   a. Ping `<the DAMP server XSI IP>`

   b. Telnet `<the DAMP server XSI IP> <monitoring port, default 9675>`

   If steps a or b fail, go to step 3.

3. `ssh admusr@<DAMP server XMI>`.

   a. Run the `sudo netstat -anop | grep <monitoring port, default 9675>` command to see if there is a TCP listen socket on that DAMP XSI IP.

   If yes, check the DAMP XSI network (hardware and software).

   If no, check the configuration of the DAMP.

1. Recovery:

1. Check the status of the application servers by navigating to the **Status & Manage**, and then **Server** page.
2. Consult the application server's documentation for recovery steps.
3. If the application server is functioning, check for network connectivity issues between the IPFE and the application server.
4. It is recommended to contact My Oracle Support if further assistance is needed.

5002 - IPFE Address Configuration Error

Alarm Group:
IPFE

Description:
This alarm indicates misconfiguration due to manual changes to the configuration database, configuration data importing errors, or software installation errors. In general, this error is caused by IPFE IP addresses being incorrectly configured.

Severity:
Critical

Instance:
Description of the field or fields that are incorrect.

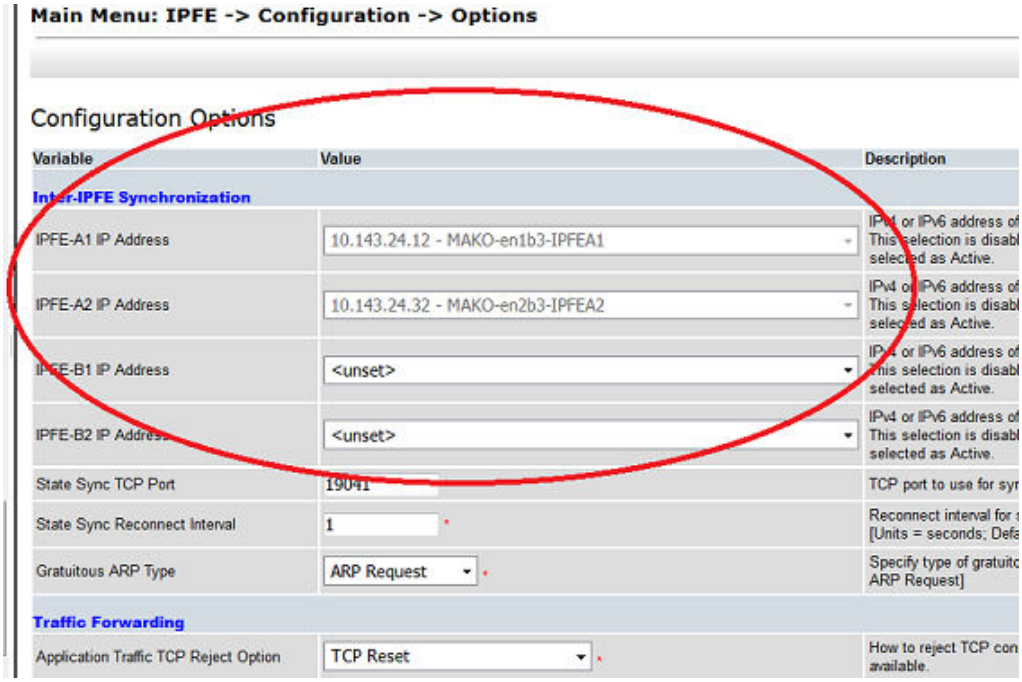
> **Note:**
>
> If the IPFE is able to successfully synchronize data with its peer, this alarm clears.

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeStateSyncConfigErrorNotify

Cause:
The alarm raises if IPFE IP addresses is configured incorrectly.



The IPFE mates state synchronization is through the connection (IPFE-A1/A2 or B1/B2 IP Address, 19041, TCP). This alarm raises when the connection is not able to be established. Following are few reasons:

- IPFE-A/B: Addresses both identical - one of the addresses is incorrect
- IPFE-A/B: Cannot open IPFE device, **/dev/recent** - xt_recent module in TPD is either missing or incorrect
- IPFE-A/B: First address bad - invalid address format
- IPFE-A/B: Second address bad - invalid address format
- IPFE-A/B: Bind error - cannot bind a socket to this interface address
- IPFE-A/B: Both addresses empty - it is not possible to leave both addresses empty when configuring from the GUI, but it is possible if data is manually entered from GCLI command

- IPFE-A/B: Only one sync address may be local - two addresses that both correspond to an interface on the same blade have been entered
- IPFE-A/B: Peer software version incompatible - the peer IPFE is on a different version

Diagnostic Information:
Collect the following data before contacting My Oracle Support for assistance:

- `iqt -pE Network>Network_$(hostname)`
- `iqt -pE L3Interface>L3Interface_$(hostname)`
- Screenshot of **Configuration**, and then **Network**, and then **Devices**, and then **<All IPFE Server Tab>**.
- `iqt -pE IpfeOption>IpfeOption_$(hostname)`
- `iqt -pE IpfeOption>IpListTsa_$(hostname)`
- Screenshot of **IPFE**, and then **Configuration**, and then **Options**.
- `tr.cat ipfe.STK>ipfeSTK_$(hostname)`
- `ifconfig>ifconfig_$(hostname)`

1. Recovery:

1. To correct configuration errors:
   - Read and understand the alarm text. This should have sufficient information to diagnose the configuration error. As a last resort.
   - Navigate to **IPFE**, and then **Configuration**, and then **Options**.
   - Check the IPFE-A1 and IPFE-A2 IP address. You also need to check IPFE-B1 and IPFE-B2 IP addresses, if you have full 4 IPFE servers. You should select INTERNALIMI IP address here. All servers have to be the same IP type.
   - Check the State Sync TCP Port. We suggest you always use the default 19041, if possible.
2. Ping the local IMI IP address.
3. Reboot the IPFE servers, if you have permission to do so.
4. If the alarm is still there, it is recommended to contact My Oracle Support for assistance. Collect this data first:
   - Screenshots for **Configuration**, and then **Network**, and then **Devices** All IPFE Server tab and **IPFE**, and then **Configuration**, and then **Options**.
   - `ifconfig>ifconfig_$(hostname)`

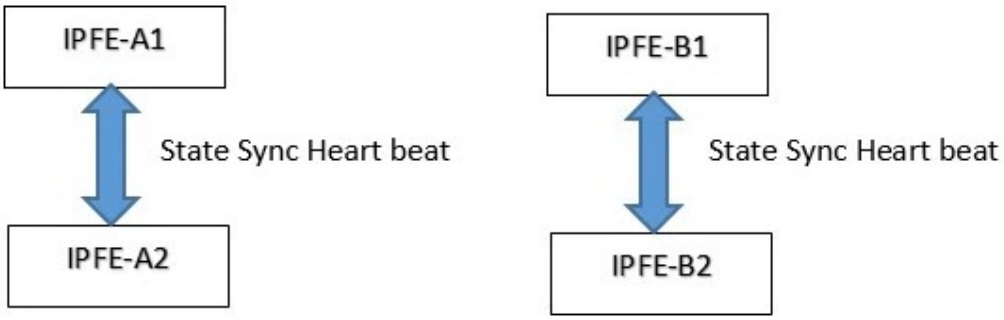
5003 - IPFE State Sync Run Error

Alarm Group:
IPFE

Description:
The IPFE was unable to synchronize state data with its mate. This alarm is generated when the IPFE server missed the heartbeat messages from its mate, or if the mate is unavailable for any reason.

This alarm is normal when one IPFE of a pair is taken down for maintenance. In this case, the alarm is guaranteed.
If the alarm is not generated, this indicates the IPFE has detected that its mate is out of service.
DSR currently supports, at most, four IPFE servers, which are named IPFE-A1, IPFE-A2, IPFE-B1, and IPFE-B2 in the **IPFE**, and then **Configuration**, and then **Options** tab. You can configure IPFE-A1 and IPFE-A2 servers only in the small DSR system and you can add IPFE-B1 and IPFE-B2 for a big size DSR, which depends on the needs. The IPFE-A1 and IPFE-A2 are configured as mated (IPFE-B1 and IPFE-B2 are mated, if configured). The heartbeat message exchanges between the mated IPFE servers once every 500ms. If, for any reason, the IPFE server missed its mate's heartbeat message, alarm 5003 is raised. A few typical reasons are:

- Mate server is down
- Network connectivity issue
- Latency between the IPFEs
- High CPU load on the IPFE causing internal software latency in the transmission or receipt of a heartbeat message



Severity:
Critical

Instance:
One of the following strings:

- connect error - cannot connect to peer IPFE
- data read error - error reading data from peer IPFE
- data write error - error writing data to peer IPFE

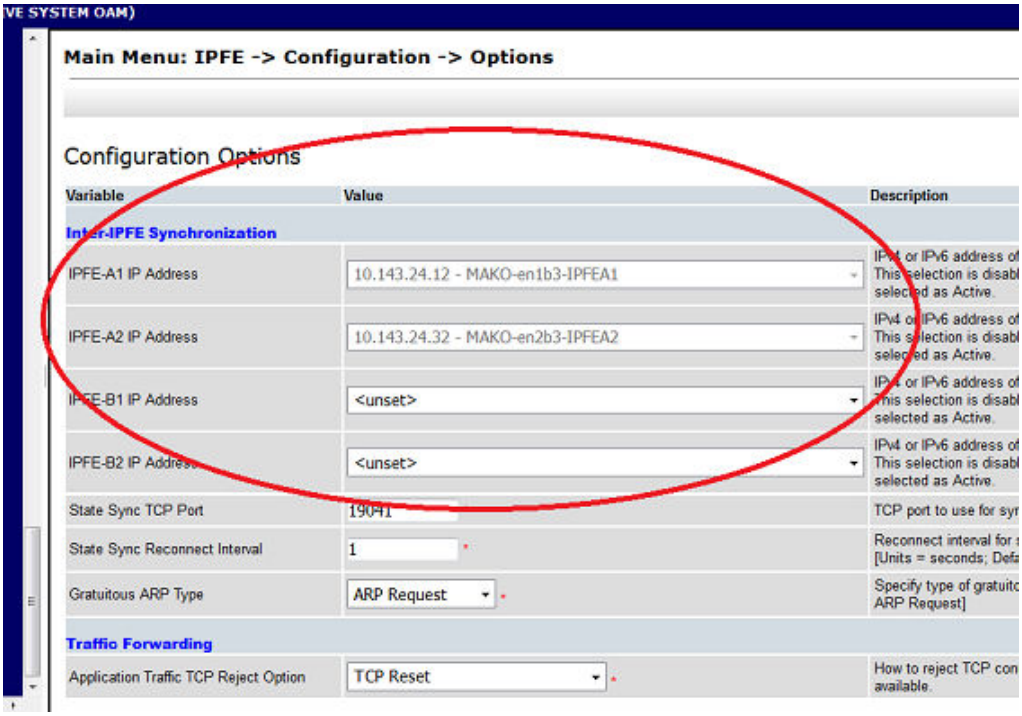
> **Note:**
> If the is able to synchronize state data with its mate, this alarm will clear.

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeStateSyncRunErrorNotify

Diagnostic Information:
The state synchronization data exchange is through the connection between IPFE server mates (IPFE A1/A2 IP or B1/B2 IP, 19041, TCP). Wireshark can be used to diagnose if there is an state sync heartbeat message sent and received.



1. Recovery:

1. Check IPFE server configurations by navigating to **IPFE**, and then **Configuration**, and then **Options** and checking the IPFE server IP address. Select the IMI IP address. The Default State Sync TCP port number is 19041. If this port number is configurable in your version of the IPFE, then do not change it from the default.
2. Check the Mated IPFE connectivity.
   - ssh to IPFE-A1. ssh admusr@<IPFE-A1 XMI IP address>
   - ping <IPFE-A2 IMI Address>
   - telnet <IPFE-A2 IMI Address> 19041
   - ssh to IPFE-A2 to ping/telnet IPFE-A1
   - ssh to IPFE-B1 to ping/telnet IPFE-B2
   - ssh to IPFE-B2 to ping/telnet IPFE-B1
   - If the mated IPFE servers are reachable to each other, go to step 3
3. Reboot the IPFE servers, one by one, if possible.
   a. Navigate to **Status & Manage**, and then **Server**.
   b. Select the IPFE server and click **Restart**.

      The **Are you sure you want to restart application software on the following server(s)? <server name>** warning message displays.

c. Click **OK** to continue.

d. If rebooting does not solve the issue or you are not allowed to reboot the IPFE server, go to the next step.

4. Do CPU and userspace performance diagnostics using the commands: `top` and `mpstat -P ALL`.

5. For further assistance, it is recommended to contact My Oracle Support for assistance. Collect this data first:

   - Screenshots of **Configuration**, and then **Network**, and then **Devices** All IPFE Server tab and **IPFE**, and then **Configuration**, and then **Options**.
   - `ifconfig>ifconfig_$(hostname)`
   - `(iqt -E IpfeOption ; iqt -E IpListTsa ; ) > ipfeconfig_$(hostname)`
   - `netstat -anop | grep 19041>netstat_$(hostname)`

5004 - IPFE IP Tables Configuration Error

Alarm Group:
IPFE

Description:
This alarm indicates misconfiguration of the Target Set due to manual changes to the configuration database or configuration data importing errors. One or more of the IP addresses configured for the application servers is not valid.

Severity:
Critical

Instance:
tsa N address misconfiguration where N is 1-16

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeIpTablesConfigErrorNotify

1. Recovery:

1. Navigate to **IPFE**, and then **Configuration**, and then **Options**.

> **Note:**
> When the target set address is configured correctly, this alarm clears.

2. From the Configuration Options screen, navigate to **IPFE**, and then **Configuration**, and then **Target Sets**.

3. Ensure there Target Set Address field contains a valid IP address.

4. Ensure there is at least one application server IP address configured in the Target Set IP List for the TSA.
5. Repeat for each TSA on the Target Set screen.

5005 - IPFE Backend In Stasis

Alarm Group:
IPFE

Description:
The IPFE has received a heartbeat packet from the application server that indicates the application server is unwilling to accept new connections. However, the application server continues to process existing connections. The application server sends a stasis heartbeat message for the following reasons:

- The application server has reached its maximum number of active Diameter connections
- The application server is congested. The application server also raises 22200 - MP CPU Congested.

Severity:
Minor

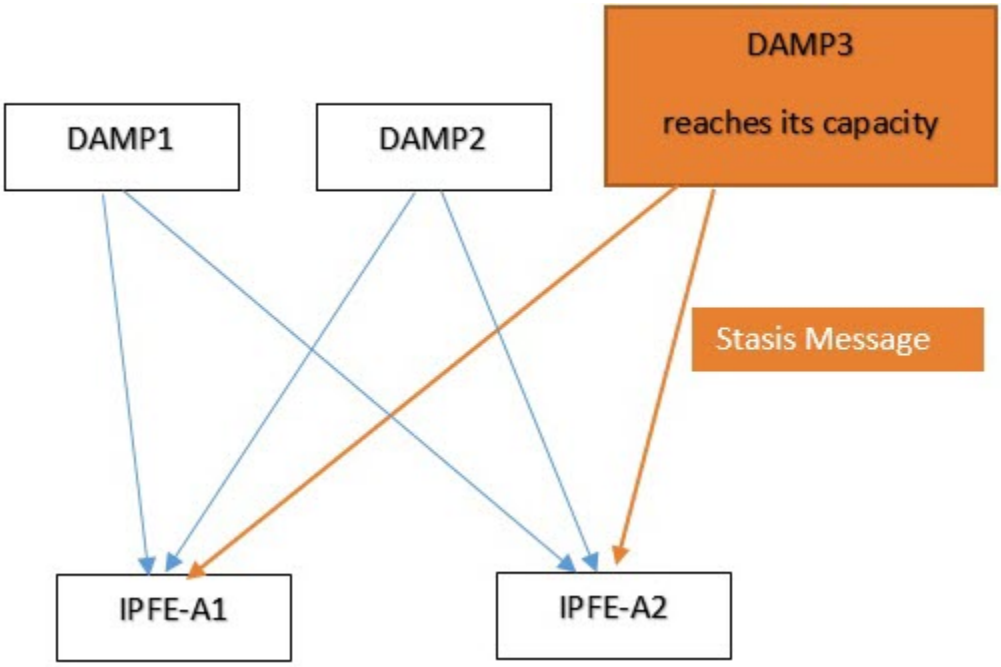
Instance:
IP address of the application server in stasis

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeBackendInStasisNotify

Cause:
The application server has reached is maximum resource capacity.
When one or more of the DAMPs in the cluster reaches its capacity. The DAMP servers that reach their capacity send Stasis messages to the IPFE servers.



When the IPFE servers received this stasis message, the IPFE will:

- Raise this 5005 alarm.
- Keep processing the existing connection to this stasis DAMP server.
- Route any NEW connection (TCP SYN, SCTP INIT) to other un-stasis servers in the cluster.

The IPFE clears this alarm when the IPFE server receives no more stasis message from the DAMP servers.
It usually means more back-end DAMP servers are required to extend the capacity when this alarm displays. Contact the Oracle support team to help diagnose the issue.

Diagnostic Information:
Collect following data before contacting Oracle Support:

1. Export the alarm history.
2. `iqt -pE IpfeOption>IpfeOption_$(hostname)`
3. `iqt -pE IpListTsa>IpListTsa_$(hostname)`
4. `ipfe.STK>ipfeStk_$(hostname)`
5. Screenshot of **Diameter**, and then **Maintenance**, and then **DA-MPs**, and then **DA-MP Connectivity**.

1. Recovery:

- When the IPFE receives heartbeats from the application server indicating it is willing to accept new connections, this alarm clears.

5006 - Error Reading from Ethernet Device. Restart IPFE Process.

Alarm Group:
IPFE

Description:
IPFE was unable to read from an ethernet device.

> **Note:**
>
> If IPFE is able to read from the ethernet device, this alarm clears.

Severity:
Critical

Instance:
pcap <ethernet device name> or network interface devices added or removed

HA Score:
Degraded

Auto Clear Seconds:
N/A

OID:
ipfeIpfeEtherDeviceReadErrorNotify

Cause:
For an old IPFE version, restart IPFE to collect the data for the DSR reconfiguration like a new added Ethernet card or a deleted bond.

1. Recovery

1. Navigate to **Status & Manage**, and then **Server**.
2. Select the IPFE server and click **Restart**.

   The **Are you sure you want to restart application software on the following server(s)? <server name>** warning message displays.
3. Click **OK** to continue.

5007 - Out of Balance: Low

Alarm Group:
IPFE

Description:
Traffic statistics reveal an application server is processing lower than average load. For example, if a TSA has three application servers, but the IPFE has only two connections open, then one of the application servers receives no traffic and thus is considered "underloaded."

Severity:
Minor

Instance:
IP address of the application server

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeBackendUnderloadedNotify

Cause:
The IPFE has an algorithm to calculate the average traffic load of the DA-MP application servers, at times the traffic on a DA-MP server may outside of the average range. When an IPFE detects DA-MPs traffic is unbalanced and processing a lower than average load, the IPFE server displays the 5007 alarm.
Few of the causes the IPFE to raise this alarm are:

- A new DA-MP server has just been added to a cluster.
- A DA-MP has just been stopped for maintenance or some other reason.
- The activated traffic rate is to low.

These alarms are not harmful to the system, and indicates the IPFE traffic on a DA-MP server is imbalanced for some reason. There is no impact to traffic or connections and this alarm does not cause disconnection or congestion. As new connections get established, and statistics indicate the server is no longer under loaded, alarm 5007 gets cleared.

Diagnostic Information:
Collect following data before contacting My Oracle Support for assistance.

1. Export alarm history.
2. `grep * /proc/net/xt_recent* > xt_recent1_$(hostname)`
3. `grep * /proc/net/xt_recent*/*> xt_recent2_$(hostname)`
4. `tr.cat ipfe.STK>ipfeSTK_$(hostname)`
5. `iqt -pE IpfeOption>IpfeOption_$(hostname)`
6. `iqt -pE IpListTsa>IpListTsa_$(hostname)`

1. Recovery:

1. None required. Underloaded application servers do not impact traffic processing. This alarm clears when traffic statistics reveal the application server is no longer underloaded.
2. It is recommended to contact My Oracle Support if further assistance is needed.

5008 - Out of Balance: High

Alarm Group:
IPFE

Description:
Traffic statistics reveal an application server is processing higher than average load and does not receive new connections.

Severity:
Minor

Instance:
IP address of the overloaded application server.

> **Note:**
>
> When traffic statistics indicate the application server is no longer overloaded, this alarm clears.

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeBackendOverloadedNotify

Cause:
The IPFE has an algorithm to calculate the average traffic load of the DA-MP application servers. At times the traffic on a DA-MP server reaches outside of the average range. When an IPFE detects DA-MPs traffic is unbalanced and processing a higher than average load, the IPFE server displays the 5008 alarm.
Few of the causes for IPFE to raise this alarm are:

- A new DA-MP server has just been added to a cluster.
- A DA-MP has just been stopped for maintenance or some other reason.
- The activated traffic rate is to high.

These alarms are not harmful to the system, and indicate the IPFE traffic on a DA-MP server is unbalanced for some reason. There is no impact to traffic or connections and this alarm does not cause disconnection or congestion. As new connections are established, and statistics indicate the server is no longer overloaded, alarm 5008 clears.

Diagnostic Information:
Collect the following DATA before contacting My Oracle Support for assistance.

1. Export alarm history.
2. `grep * /proc/net/xt_recent* > xt_recent1_$(hostname).`

3. `grep * /proc/net/xt_recent*/*> xt_recent2_$(hostname).`
4. `tr.cat ipfe.STK>ipfeSTK_$(hostname).`
5. `iqt -pE IpfeOption>IpfeOption_$(hostname).`
6. `iqt -pE IpListTsa>IpListTsa_$(hostname).`

1. Recovery:

1. IPFE monitors traffic statistics and does not assign connections to the overloaded application server until statistics indicate the server is no longer overloaded.
2. Check the status of the application servers by navigating to the **Status & Manage**, and then **Server** page.
3. Consult the application server's documentation for recovery steps.
4. It is recommended to contact My Oracle Support if further assistance is needed.

5009 - No Available Servers in Target Set

Alarm Group:
IPFE

Description:
Through monitoring of the application servers, the server learns no server in a target set is available. The associated measurement, TxReject, also shows counts (refer to the *DSR Measurements Reference* for details about this measurement). This alarm can be triggered during configuration of the IPFE when the target set address has been configured, but application servers have not yet been added to the target set. Setting the Monitoring Connection Timeout to a value less than 2 seconds is the primary cause of this alarm. It is recommended to leave this setting on the default of 3 seconds. Do not set to 1 second. Later releases prohibit this from being set to 1 second.
Each target set is configured with at least one backend application server (DAMP). The IPFE raises the 5009 alarm when the IPFE detects no DAMP is live. The IPFE detects the DAMP liveliness by receiving the DAMP heartbeat on time.

Severity:
Critical

Instance:
tsa N has no available servers where N is 1-16

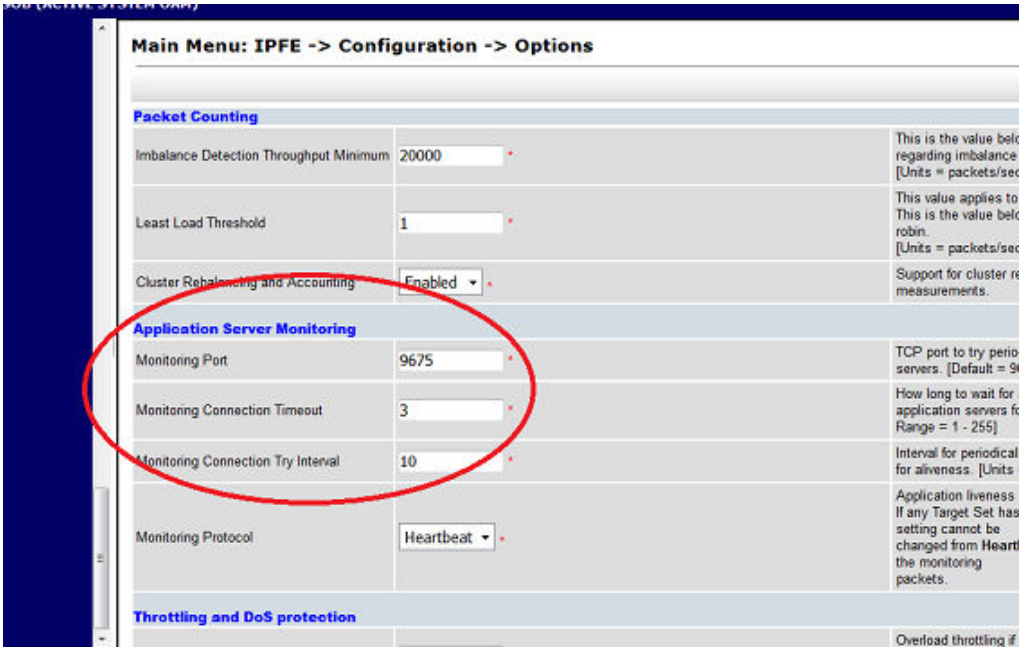
> **Note:**
>
> When at least one application server in a target set becomes available, this alarm clears.

HA Score:
Normal

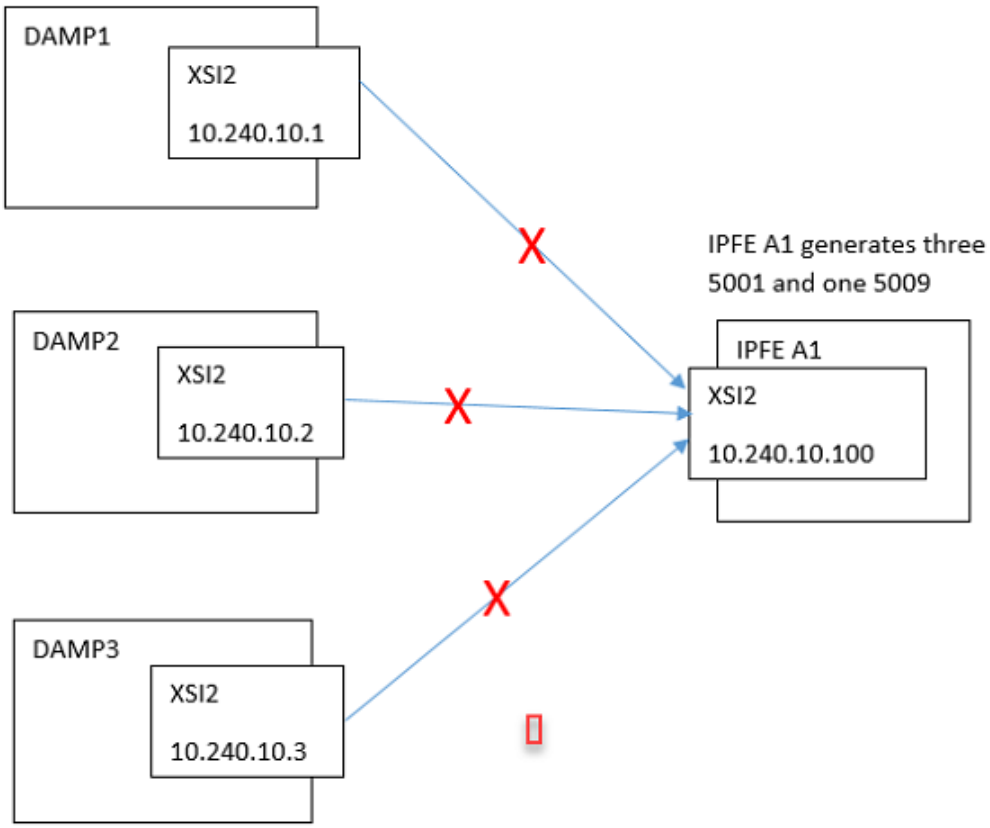
Auto Clear Seconds:
N/A

OID:
ipfeIpfeNoAvailableAppServersNotify

Cause:
Setting the Monitoring Connection Timeout to a value less than 2 seconds is the primary cause of this alarm. It is recommended to leave this setting on the default of 3 seconds. Do not set to 1 second. Later releases prohibit this from being set to 1 second.
Each target set is configured with at least one backend application server (DAMP). The IPFE raises the 5009 alarm when the IPFE detects no DAMP is live. The IPFE detects the DAMP liveliness by receiving the DAMP heartbeat on time. The following screen shows the IPFE monitoring the DAMP XSI port 9675 and the heartbeat is received every 3 seconds through this port.



When the IPFE does not receive the heartbeat from a single backend DAMP the IPFE raises alarm 5001. When the IPFE does not receive the heartbeat for all backend DAMPs in its TSA List, the IPFE raises the alarm 5009.
When 5009 alarm raises, the IPFE is not able to route the connection to a backend DAMP server. This alarm is critical.
For example:
TSA1 10.240.10.162 has three backend DAMPs (DAMP1-XSI2-10.240.10.1, DAMP2-XSI2-10.240.10.2, and DAMP3-XSI2-10.240.10.3), when IPFE is not able to receive the heartbeat in time from DAMP1, alarm 5001 raises from its active IPFE server. When IPFE misses all three DAMP heartbeats, alarm 5009 raises from its active IPFE server.



Diagnostic Information:
The Wireshark is the normal tool to monitor if the DAMP is sending a heat beat to IPFE. Follow these steps to diagnose the issues:

1. From the SO GUI, navigate to **IPFE**, and then **Configuration**, and then **Target Sets**, and then **TSA#**, and then **+**; at least one DAMP server XSI IP should be present. If yes, go to step 2.
2. Log into the IPFE server. - ping `<the DAMP server XSI IP>` - `telnet <the DAMP server XSI IP> <monitoring port, default 9675>`. If fail, go to step 3.
3. `ssh admusr@<DAMP server XMI>`. Run the `sudo netstat -anop | grep <monitoring port, default 9675>` command to see if there is a TCP listen socket on that DAMP XSI IP. If no, check the configuration of the DAMP. If yes, check the DAMP XSI network (hardware and software).

1. Recovery:

1. Make sure the Monitoring Connection Timeout setting is not less than 2 seconds. Change to a higher value, if required
2. From the SO GUID, navigate to **IPFE**, and then **Configuration**, and then **Target Sets**. At least on DAMP server XSI IP address should display.
3. Log into the IPFE server.
   - ssh to admusr@ @<IPFE XMI IP>
   - ping <the DAMP server XSI IP>
   - telnet <the DAMP server XSI IP> <monitoring port, default 9675>

The telnet terminal prints gibberish at even intervals. These are the raw heartbeat messages. If you see nothing, then the DSR is not sending hearbeats.

- ssh to admusr@ @<DAMP server XMI>
- sudo netstat -anop | grep <monitoring port, default 9675> to see if there is a TCP listen socket on the DAMP XSI IP
  If no, check the configuration of the DAMP

  If yes, check the DAMP XSI network (switch/firewall...)

4. If application servers have been configured correctly for the target set and the application server status is healthy, it is recommended to contact My Oracle Support for assistance. Collect this data first:
   - Screenshot of **IPFE**, and then **Configuration**, and then **Target Sets** edit screen.
   - `ifconfig>ifconfig_$(hostname)`
   - `cat /etc/sysconfig/network > network_$(hostname)`
   - `cat /etc/modeprobe.d/bnx2x.conf > bnx2x.conf_$(hostname)`
   - `cat /etc/sysconfig/network-scripts/ifcfg-eth01`

5010 - Unknown Linux iptables Command Error

Alarm Group:
IPFE

Description:
The IPFE received an unknown error parsing Linux iptables output. This internal software error is generated when the iptables kernel module is updated and provides an error the IPFE wasn't coded to handle. It occurs during startup, if it occurs at all.

Severity:
Critical

Instance:
error parsing iptables output

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeErrorParsingIptablesOutputNotify

1. Recovery:

- The alarm clears when the kernel output from the iptables command is parsable. If the problem persists, collect the following data and it is recommended to contact My Oracle Support for assistance.
  - From the active NO/SO GUI, navigate to **Status & Manage**, and then **Server**.

- From the Server Status screen, select the IPFE to stop (as it occurs during startup) and click **Stop**.
- Log into the IPFE blade as root.
- Make a directory for holding data: `# mkdir /var/TKLC/db/filemgmt/<data_collection_directory>`
- Change to that directory.
- Issue the following commands with root account:
  # /sbin/iptables -vxZ -t filter -nL > iptables_filter.txt

  # /sbin/iptables -vxZ -t mangle -nL > iptables_mangle.txt

  # /sbin/ip6tables -vxZ -t filter -nL > ip6tables_filter.txt

  # /sbin/ip6tables -vxZ -t mangle -nL > ip6tables_mangle.txt
- tar and compress the directory.
- From the active NO/SO GUI, navigate to **Status & Manage**, and then **Server** and restart IPFE.

5011 - System or Platform Error Prohibiting Operation

Alarm Group:
IPFE

Description:
An internal software error. An IPFE attempt to interact with the TPD operating system has produced a fatally abnormal result (e.g., no network interfaces are provisioned on the system). This alarm is raised during startup by the following conditions:

- The IPFE cannot write to its Ethernet devices (denoted by the instances, error opening ethernet listeners or no network cards found).
- The IPFE receives an unknown error when accessing its Ethernet devices.
- The issuance of the service network restart command.
- The IPFE cannot assign Ethernet device queues to certain CPUs, which is denoted by the instance, Cannot update /proc/irq/N/smp_affinity setting.

Severity:
Critical

Instance:
Description of the problem.

- Error opening ethernet listeners
- No network cards found
- Cannot update `/proc/irq/N/smp_affinity setting`
- System has less than 16 CPUs

> **Note:**
>
> The IPFE detects if it has been installed on a virtual machine and will not raise this alarm.

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
ipfeIpfeSystemErrorNotify

1. Recovery:

1. If the IPFE is able to use its ethernet interfaces, this alarm will clear. If this alarm was generated by issuing a service network restart command, it should clear within 10 seconds. If it does not clear, restart the IPFE process:
   a. Select **Status & Manage**, and then **Server**.
   b. Select the IPFE server and click **Restart**.

      The **Are you sure you want to restart application software on the following server(s)? <server name>** warning message displays.
   c. Click **OK** to continue.
2. If the alarm still does not clear, check the Ethernet devices and CPUs.
3. It is recommended to contact My Oracle Support if further assistance is needed.

5012 - Signaling Interface Heartbeat Timeout

Alarm Group:
IPFE

Description:
Heartbeats to monitor the liveness of a signaling interface have timed out. IPFE always monitors the working condition of its mate signaling interfaces(XSI) as an entirely separate monitoring mechanism to the synchronization channel. This is done by the IPFE server sends the heartbeat message to its mate through the signaling interfaces(XSI) using the default UDP port 19041. If the heartbeat is not received in 3000ms, then the IPFE server assumes the signaling interface is out of service, and takes over traffic from its mate. At the same time the IPFE raises the alarm 5012 .

Severity:
Critical

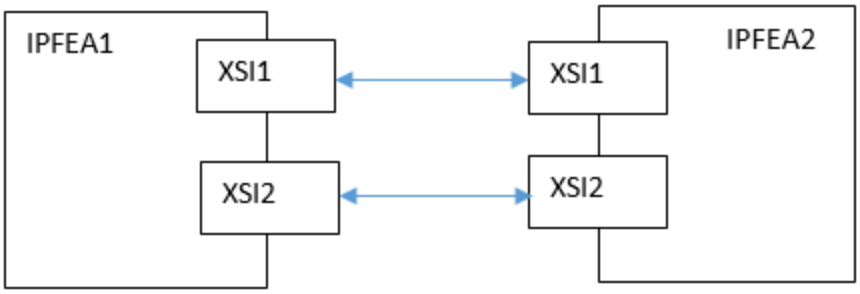
Instance:
The name of the Ethernet interface affected, for example, bond0.5.

HA Score:
Degraded

Auto Clear Seconds:
N/A

OID:
ipfeIpfeSignalingInterfaceNotify

Cause:
Following is the example for the heartbeat message exchange between the IPFE mates.



Diagnostic Information:
This alarm is normal for the situation where one IPFE of a mated pair has been taken down for maintenance. This alarm only needs to be acted upon if it is raised when both IPFEs are expected to be available.

1. From the alarm report to determine the issue interface (`eth01`, `bond0.313` and so on). For example, when the alarm instance shows: `IPFEA1:bond0.313`. The issue interface shall be `IPFEA2 (mate),bond0.313`.
2. Then using the Wireshark to monitor if the Heartbeat messages is sent from `IPFEA2, bond0.313` (no need to look into the message). If no, the issue is on IPFEA2. If yes, the issue shall be in the network.

1. Recovery:

1. Check if any manual configuration changes have been executed that removed or reset interfaces.
2. Diagnose hardware failure of interfaces, switch failure, or network outage when the issue is on the network.
3. Review currently active platform alarms.
4. It is recommended to contact My Oracle Support if further assistance is needed.

5013 - Throttling Traffic

Alarm Group:
IPFE

Description:
IPFE has seen traffic in excess of Global Packet Rate Limit and is dropping packets to throttle the traffic. To protect the DSR, IPFE defines a Global Packet Rate Limit set as a ingress signaling traffic rate throttle. The packet rate is accounted for on a per-local-port bases, thus each separate DSR listening port can receive each the default of 500,000 packets/second. When the IPFE is processing traffic in excess of this rate, the IPFE throttles the traffic by smoothly dropping packets in the manner of

an overloaded border router. The default value of this rate throttle is 500,000 packets/second.
When traffic is approaching or exceeding its overload capacity, the alarm 5100 is raised and does not drop the packets. But when the traffic reaches this throttle, IPFE drops the packets

Severity:
Critical

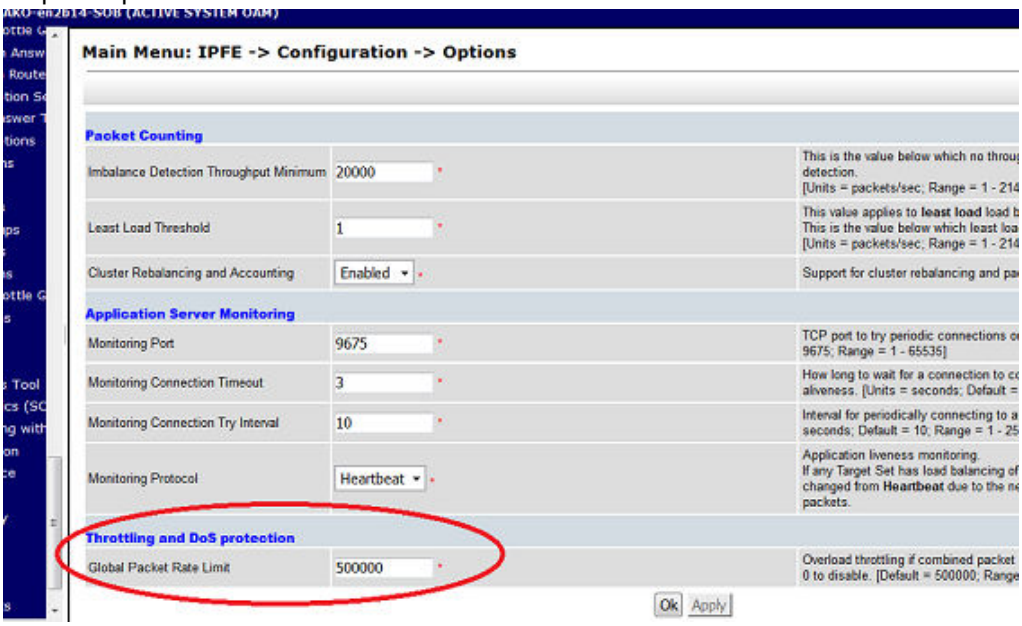
Instance:
The number of packets that have been throttled

HA Score:
Degraded

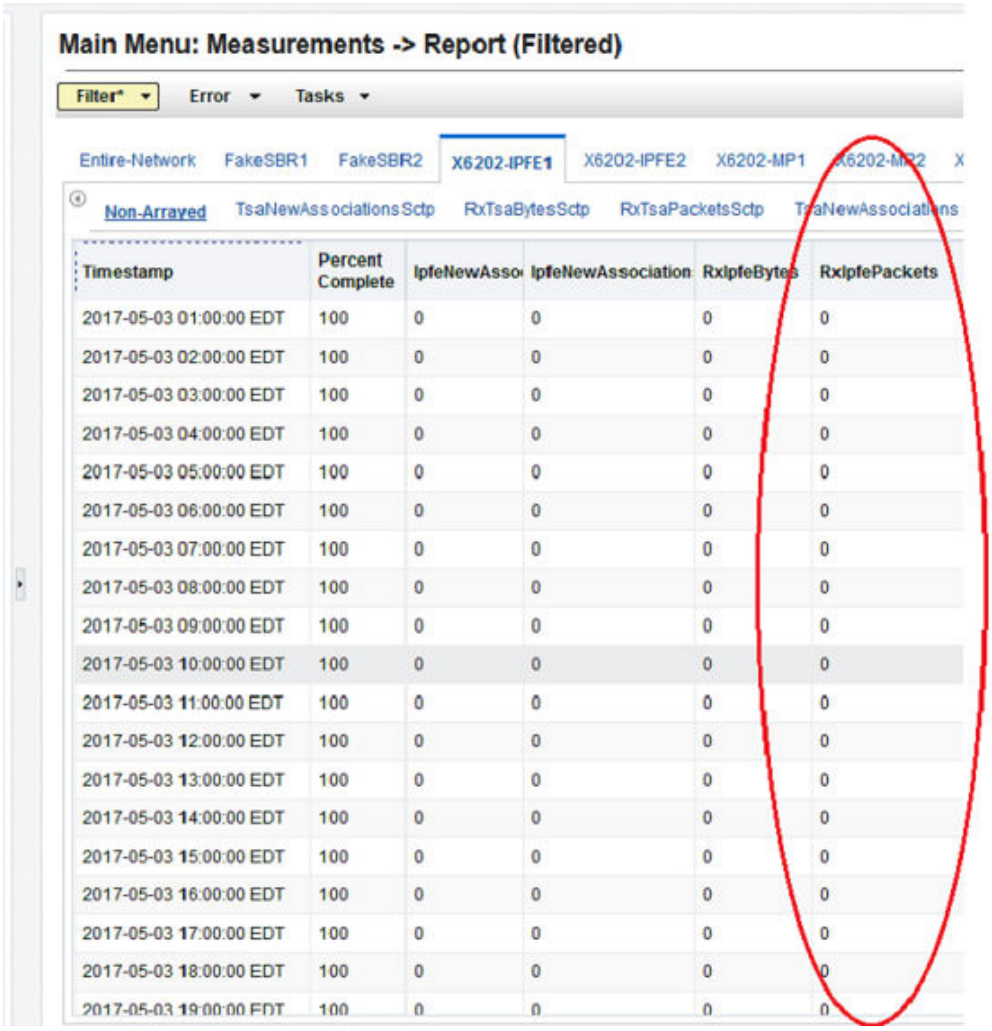
Auto Clear Seconds:
N/A

OID:
ipfeIpfeThrottlingTrafficNotify

Cause:
When traffic is approaching or exceeding its overload capacity, the alarm 5100 is raised and does not drop the packets. But when the traffic reaches this throttle, IPFE drops the packets.



Diagnostic Information:
Refer to the IPFE and connection performance to make further investigation.



1. Recovery:

1. If no packets have been dropped for five seconds, the alarm clears.
2. It is recommended to contact My Oracle Support if further assistance is needed.

5100 - Traffic Overload

Alarm Group:
IPFE

Description:
Total IPFE signaling traffic rate is approaching or exceeding its engineered capacity. IPFE defined a engineering capacity to monitoring the ingress signaling traffic rate. This alarm is raised when the total IPFE signaling traffic rate is approaching or exceeding its engineered capacity. This alarm is different to the alarm 5013, No packages drop at this point.
The severity thresholds are:

- Minor: set at 245 MB/second, clear at 220 MB/second

- Major: set at 327 MB/second, clear at 302 MB/second
- Critical: set at 409 MB/second, clear at 384 MB/second

Severity:
Minor, Major, Critical

Instance:
N/A

> **Note:**
>
> If the signaling traffic declines below the clear threshold, the alarm clears.

HA Score:
Normal

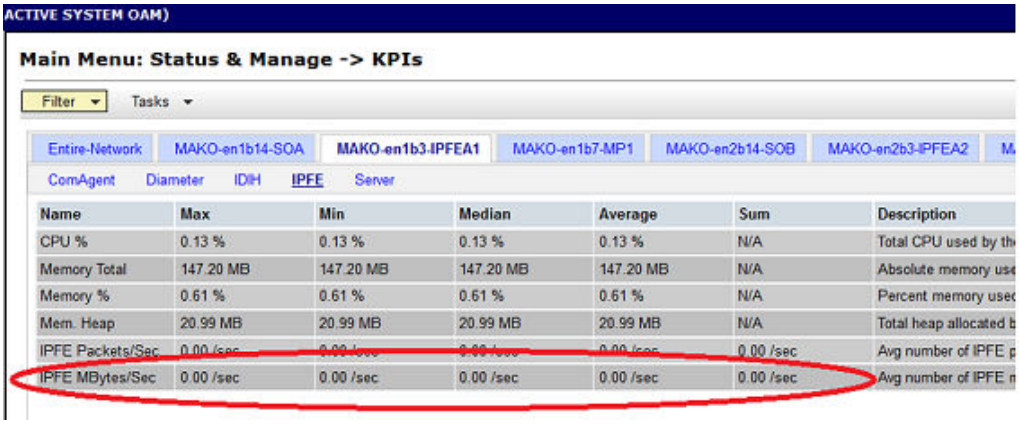
Auto Clear Seconds:
N/A

OID:
ipfeIpfeTrafficOverloadNotify

Cause:
The severity thresholds are:

- Minor: set at 245 MB/second, clear at 220 MB/second
- Major: set at 327 MB/second, clear at 302 MB/second
- Critical: set at 409 MB/second, clear at 384 MB/second

Diagnostic Information:
Refer to the KPI to check the IPFE data rate:



1. Recovery:

1. The application is in excess of its design parameters, and may exhibit traffic loss if an additional failure occurs. Consider expanding system to accommodate additional capacity.
2. It is recommended to contact My Oracle Support if further assistance is needed.

5101 - CPU Overload

Alarm Group:
IPFE

Description:
CPU utilization is approaching maximum levels.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ipfeIpfeCpuOverloadNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

5102 - Disk Becoming Full

Alarm Group:
IPFE

Description:
Disk space utilization is approaching maximum levels.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ipfeIpfeDiskUsageNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

5103 - Memory Overload

Alarm Group:
IPFE

Description:
IPFE memory utilization is approaching maximum levels.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ipfeIpfeMemoryOverloadNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

OAM (10000-10999)

This section provides information and recovery procedures for OAM alarms, ranging from 10000-10999.

10001 - Database Backup Started

Alarm Group:
DB

Description:
The database backup has started.

Severity:
Info

Instance:
GUI

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecBackupStartNotify

1. Recovery:

- No action action required.

10002 - Database Backup Completed

Alarm Group:
DB

Description:
Backup completed

Severity:
Info

Instance:
GUI

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecBackupCompleteNotify

1. Recovery:

- No action required.

10003 - Database Backup Failed

Alarm Group:
DB

Description:
The database backup has failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecBackupFailNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10004 - Database Restoration Started

Alarm Group:
DB

Description:
The database restoration has started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecRestoreStartNotify

1. Recovery:

- No action required.

10005 - Database Restoration Completed

Alarm Group:
DB

Description:
The database restoration is completed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecRestoreCompleteNotify

1. Recovery:

- No action required.

10006 - Database Restoration Failed

Alarm Group:
DB

Description:
The database restoration has failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecRestoreFailNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10008 - Database Provisioning Manually Disabled

Alarm Group:
DB

Description:
Database provisioning has been manually disabled.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
tekelecProvisioningManuallyDisabledNotify

1. Recovery:

- No action required.

10009 - Config and Prov DB Not Yet Synchronized

Alarm Group:
REPL

Description:
The configuration and provisioning databases are not yet synchronized. The 10009 alarm raises when DB re-initialization is attempted but fails. The re-initialization usually happens when transitioning to *A* state (one of the procmgr states, can get it from the `pl` command). DB re-initialization fails because the remote server is not in the correct state, for example, it is not in the OOS state.
This alarm can also be observed during some DSR patch installations after the DB replication is inhibited. As long as this alarm is cleared (NOT stuck) after DB replication is allowed, it is normal behavior and we expect to see the 10009 alarm when applying a patch.

Severity:
Critical

Instance:
N/A

HA Score:
Failed

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTCfgProvDbNoSync

Diagnostic Information:
Perform the following to diagnose the alarm:

- Examine the `/var/TKLC/appw/logs/Process/apwSoapServer.log` file on primary NO and possibly the remote server to investigate the reasons for failure.
- Software release information.

1. Recovery:

1. Monitor the replication status by navigating to **Status & Manage**, and then **Replication GUI**.
2. If alarm persists immediately after an upgrade, reboot the server once using the `sudo init 6` command on the effected server.
3. If alarm persists for more than one hour, it is recommended to contact My Oracle Support if further assistance is needed.

10010 - Stateful DB from Mate Not Yet Synchronized

Alarm Group:
HA

Description:
The stateful database is not synchronized with the mate database.

Severity:
Minor

Instance:
N/A

HA Score:
Degraded

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTStDbNoSyncNotify

1. Recovery:

- If alarm persists for more than 30 seconds, it is recommended to contact My Oracle Support if further assistance is needed.

10011 - Cannot Monitor Table

Alarm Group:
OAM

Description:
Monitoring for table cannot be set up.

Severity:
Major

Instance:
N/A

HA Score:
Degraded

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTCantMonitorTable

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10012 - Table Change Responder Failed

Alarm Group:
OAM

Description:
The responder for a monitored table failed to respond to a table change.

Severity:
Major

Instance:
N/A

HA Score:
Degraded

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTResponderFailed

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10013 - Application Restart in Progress

Alarm Group:
HA

Description:
An application restart is in progress.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTApplSWDisabledNotify

1. Recovery:

- If duration of alarm is greater than two seconds, it is recommended to contact My Oracle Support if further assistance is needed.

10020 - Backup Failure

Alarm Group:
DB

Description:
Database backup failed.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
apwBackupFailureNotify

1. Recovery:

1. Alarm clears if a backup (Automated or Manual) of the same group data is successful.
2. It is recommended to contact My Oracle Support if further assistance is needed.

10050 - Resource Audit Failure

Alarm Group:
AUD

Description:
Database backup failed.

Severity:
Minor

Instance:

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7TekelecResourceAuditFailureNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10051 - Route Deployment Failed

Alarm Group:
AUD

Description:
An error occurred in the deployment of a network. A SOAP request from route audit thread of apwSoapServer process to the TpdProvD service failed to delete the old record when *insert new route* or *update existed network route*. The audit happens every minute. The alarm gets cleared when *insert new route* or *update existed network route* record is successful.

Severity:
Minor

Instance:
Route ID failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7TekelecRouteDeploymentFailedNotify

1. Recovery:
1. Check the following on the affected server:
   - See if any network route is configured on the server (output of 'route' command).
   - Check the `iqt -Ep NetworkRoute` from active NOAM server to see if any network route is configured.
   - Check the `iqt -Ep ResourceAudit.1` from active NOAM server to see if any network route is in audit.
   - Check if the apwSoapServer service is running (output of `pl` command).
   - Check if the tpdProvd service is running (output of `top` or `ps` command).
   - Check if there is any SOAP error in the following log files:
     - `/var/TKLC/appw/logs/Process/apwSoapServer.log`
     - `/var/TKLC/log/tpdProvd/tpdProvd.log`
   - Try to identify if the problem occurred in tpdProvd or apwSoapServer.
2. Try restarting the apwSoapServer service on the affected server.
3. If the alarm persists, collect trace list in Diagnostic Information and it is recommended to contact My Oracle Support if further assistance is needed.

10052 - Route Discovery Failed

Alarm Group:
AUD

Description:
An error occurred in the discovery of network routes. A SOAP request from route audit thread of apwSoapServer process to the TpdProvD service failed to get the list and details of the configured network routes. The audit happens every minute. The alarm gets cleared when the route information is received from the TpdProvD service.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7TekelecRouteDiscoveryFailedNotify

1. Recovery:
1. Check the following on the affected server:
   - See if any network route is configured on the server (output of 'route' command)
   - Check if the apwSoapServer service is running (output of 'pl' command)
   - Check if the tpdProvd service is running (output of 'top' or 'ps' command)
   - Check if there is any SOAP error in the following log files:
     - `/var/TKLC/appw/logs/Process/apwSoapServer.log`
     - `/var/TKLC/log/tpdProvd/tpdProvd.log`
   - Try to identify if the problem occurred in tpdProvd or apwSoapServer
2. Try restarting the apwSoapServer service on the affected server.
3. It is recommended to contact My Oracle Support if further assistance is needed.

10053 - Route Deployment Failed - No Available Device

Alarm Group:
AUD

Description:
A suitable device could not be identified for the deployment of a network route.

Severity:
Minor

Instance:
Route ID that failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7TekelecNoRouteDeviceNotify

Cause:
AppWorks audit tries to insert, edit, or delete a route for a device which does not exist. The audit happens every minute. The alarm clears when the AppWorks audit is able to insert, edit, or delete the route.

Diagnostic Information:
Check the following on the affected server:

- Check the `iqt -Ep ResourceAudit.1` from active NOAM server to see if any network route is in audit.
- Find the device for the route.
- If the device specified is other than auto, check the user interface to see if the specified device is present.
- Check apwSoapServer logs for more information.

1. Recovery:
1. If the device specified is AUTO:
   a. Deploy the route on a specific device instead of using the “AUTO” device.
   b. Ensure every server in the server group has a usable device for the selected gateway.
2. If the device specified is deleted:
   a. Recreate the missing device.
   b. Wait for audit to re-run which shall configure the route and clear the alarm.

10054 - Device Deployment Failed

Alarm Group:
AUD

Description:
An error occurred in the deployment of a network device.

Severity:
Minor

Instance:
Device name that failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7TekelecDeviceDeploymentFailedNotify

Cause:

- Device Audit attempted to update a configured network interface device in the system configuration using the TpdProvD soap service which returned failure.
- Apart from any platform related issue like TpdProvD SOAP service not being ready, invalid input is the main cause of this alarm.

Diagnostic Information:
If device is added through one of the configuration interfaces, verify the device configuration file, `/etc/sysconfig/network-scripts/ifcfg-<dev>` is not already present.
If the device is edited through one of the configuration interfaces, verify the device configuration file, `/etc/sysconfig/network-scripts/ifcfg-<dev>` is present and is not RCS locked.
To determine the cause, look for errors in following files:

- **/var/TKLC/log/tpdProvd/tpdProvd.log**
- **/var/TKLC/appw/logs/Process/apwSoapServer.log**

1. Recovery:

1. If device is added using one of the configuration interfaces, delete any /etc/sysconfig/network-scripts/ifcfg-<dev> for the device if present.
2. If the device is edited using one of the configuration interfaces:
   a. if the `/etc/sysconfig/network-scripts/ifcfg-<dev>` is missing, then add the device using netAdm command.
   b. if the `/etc/sysconfig/network-scripts/ifcfg-<dev>` is RCS locked, use rcstool command to RCS unlock the file.
3. Delete the device, wait for the alarm to clear and then add it back.
4. It is recommended to contact My Oracle Support if further assistance is needed.

10055 - Device Discovery Failed

Alarm Group:
AUD

Description:
An error occurred in the discovery of network devices. No network device could not found; more specifically, if the `/etc/sysconfig/network` scripts directory could not be read by the apwSoapServer audit; or 1 named network device could not be

discovered on the system, more specifically, if the `/sbin/ip addr show <dev>` command fails when run from the apwSoapServer audit.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7TekelecDeviceDiscoveryFailedNotify

1. Recovery:

1. Correct any directory or file permissions in the `/etc/sysconfig/network-scripts/*` directory. It should be 0755 or relaxed.
2. Check if the named device interface is configured, that is, the interface files (ifcfg-<dev>) are present in the `/etc/sysconfig/network` scripts directory.
3. If the physical device is present on the system, but it does not show up in the output of ifconfig command, then use the `netAdm` command to add the device to the platform configuration.
4. It is recommended to contact My Oracle Support if further assistance is needed.

10073 - Server Group Max Allowed HA Role Warning

Alarm Group:
HA

Description:
The server group has received the maximum number of allowed HA role warnings.

Severity:
Minor

Instance:
Affected Server Group name

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
oAGTSgMaxAllowedHARoleWarnNotify

1. Recovery:

1. Log into the SO GUI and navigate to the **Status & Manage**, and then **HA**.

2. Click **Edit** and change the Max Allowed HA role of the current Standby SOAM to *Active*.
3. If you cannot perform the HA switchover, log into the server (**Status & Manage**, and then **Server**).
4. Select the active server and click **Restart** to restart the server.

   HA switchover occurs.
5. Verify the switchover was successful from the active SOAM GUI, or log into the active and standby SOAMs and execute this command:

   ```
   # ha.mystate
   ```

10074 - Standby Server Degraded While Mate Server Stabilizes

Alarm Group:
HA

Description:
The standby server has temporarily degraded while the new active server stabilizes following a switch of activity.

Severity:
Minor

Instance:
N/A

HA Score:
Degraded

Auto Clear Seconds:
This alarm does not autoclear.

OID:
hASbyRecoveryInProgressNotify

1. Recovery:

- No action required. The alarm clears automatically when the standby server is recovered. This is part of the normal recovery process for the server that transitioned to standby as a result of a failover.

10075 - Application Processes Have Been Manually Stopped

Alarm Group:
HA

Description:
The server is no longer providing services because application processes have been manually stopped.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not clear automatically.

OID:
hAMtceStopApplicationsNotify

1. Recovery:

- If maintenance actions are complete, restart application processes on the server from the **Status & Manage**, and then **Servers** and selecting **Restart Applications** for the server that raised the alarm.

  Once successfully restarted, the alarm clears.

10078 - Application Not Restarted on Standby Server Due to Disabled Failure Cleanup Mode

Alarm Group:
HA

Description:
The applications on the standby server have not been restarted after an active-to-standby transition since *h_FailureCleanupMode* is set to 0.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
failureRecoveryWithoutAppRestartNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10100 - Log Export Started

Alarm Group:
LOG

Description:
Log files export operation has started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportStartNotify

1. Recovery:

- No action required.

10101 - Log Export Successful

Alarm Group:
LOG

Description:
The log files export operation completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportSuccessNotify

1. Recovery:

- No action required.

10102 - Log Export Failed

Alarm Group:
LOG

Description:
The log files export operation failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportFailedNotify

1. Recovery:

1. Verify the export request and try the export again.
2. It is recommended to contact My Oracle Support if further assistance is needed.

10103 - Log Export Already in Progress

Alarm Group:
LOG

Description:
Log files export operation did not run; an export can only run on an active network OAMP server.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportNotRunNotify

1. Recovery:

- Restart the export operation after existingan export completes.

10104 - Log Export File Transfer Failed

Alarm Group:
LOG

Description:
The performance data export remote copy operation failed.

Severity:
Info

Instance:
<Task ID>

> **Note:**
>
> <Task ID> refers to the ID column found in **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecExportXferFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10105 - Log Export Cancelled - User Request

Alarm Group:
LOG

Description:
The log files export operation cancelled by user.

Severity:
Info

Instance:
<Task ID>

> **Note:**
>
> <Task ID> refers to the ID column found in **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportCancelledUserNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10106 - Log Export Cancelled - Duplicate Request

Alarm Group:
LOG

Description:
The log files export operation was cancelled because a scheduled export is queued already.

Severity:
Info

Instance:
<Task ID>

> **Note:**
>
> <Task ID> refers to the ID column found in **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportCancelledDuplicateNotify

1. Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. It is recommended to contact My Oracle Support if further assistance is needed.

10107 - Log Export Cancelled - Queue Full

Alarm Group:
LOG

Description:
The log files export operation cancelled because the export queue is full.

Severity:
Info

Instance:
<Task ID>

> **Note:**
>
> <Task ID> refers to the ID column found in **Status & Manage**, and then **Tasks**, and then **Active Tasks**.

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogExportCancelledQueueNotify

1. Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.
2. It is recommended to contact My Oracle Support if further assistance is needed.

10108 - Duplicate Scheduled Log Export Task

Alarm Group:
LOG

Description:
A duplicate scheduled log export task has been queued.

Severity:
Minor

Instance:
<Target ID>

> **Note:**
>
> <Target ID> refers to the scheduled task ID found by running a report from **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
tekelecLogExportDupSchedTaskNotify

1. Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. It is recommended to contact My Oracle Support if further assistance is needed.

10109 - Log Export Queue is Full

Alarm Group:
LOG

Description:
The log export queue is full

Severity:
Minor

Instance:
<Queue Name>

> **Note:**
>
> <Queue Name> refers to the name of the queue used for the export task ID found by running a report from either **Status & Manage**, and then **Tasks**, and then **Active Tasks** or **Status & Manage**, and then **Tasks**, and then **Scheduled Tasks**.

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
tekelecLogExportQueueFullNotify

1. Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.
2. It is recommended to contact My Oracle Support if further assistance is needed.

10110 - Certificate About to Expire

Alarm Group:
AUD

Description:
The certificate expires within 30 days.

Severity:
Minor

Instance:
<CertificateName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
certificateAboutToExpire

Cause:
The certificate is expired.

Certificate Management
The Certificate Management feature allows users to configure certificates for:

- **HTTPS/SSL** - Allows secure login without encountering messages about untrusted sites
- **LDAP (TLS)** - Allows the LDAP server's public key to encrypt credentials sent to the LDAP server
- **TLS/DTLS over TCP/SCTP Transport** - Allows transport layer security protocols and encryption on a per connection basis at the application layer. For example, DSR local and peer node connections
- **Single Sign-On (SSO)** - Allows users to navigate among several applications without having to re-enter login credentials
- **Certificate Authority (CA)** - A digital certificate provided by a trusted source used to make secure connections between a client and server

> **Note:**
>
> When setting up Certificate Management, you must first assign a system domain name for the DNS configuration before importing any certificates.

If you allow a certificate to expire, the certificate becomes invalid, and you are no longer able to run secure transactions on your website. The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date.

Diagnostic Information:
Generating a Certificate Report

To generate a certificate report:

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.
2. Select the certificate for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold `Ctrl` as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

1. Recovery:

1. For details on DNS Configuration feature, see the DNS Configuration chapter in *Operation, Administration, and Maintenance (OAM) Guide*.
2. For details on Certificate Management feature, see the Certificate Management chapter in *Operation, Administration, and Maintenance (OAM) Guide*.
3. It is recommended to contact My Oracle Support if further assistance is needed.

10111 - Certificate Expired

Alarm Group:
AUD

Description:
The certificate is expired.

Severity:
Major

Instance:
<CertificateName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
certificateExpired

Cause:
The certificate is expired.

Certificate Management
The Certificate Management feature allows users to configure certificates for:

- **HTTPS/SSL** - Allows secure login without encountering messages about untrusted sites
- **LDAP (TLS)** - Allows the LDAP server's public key to encrypt credentials sent to the LDAP server

- **TLS/DTLS over TCP/SCTP Transport** - Allows transport layer security protocols and encryption on a per connection basis at the application layer. For example, DSR local and peer node connections
- **Single Sign-On (SSO)** - Allows users to navigate among several applications without having to re-enter login credentials
- **Certificate Authority (CA)** - A digital certificate provided by a trusted source used to make secure connections between a client and server

> **Note:**
>
> When setting up Certificate Management, you must first assign a system domain name for the DNS configuration before importing any certificates.

If you allow a certificate to expire, the certificate becomes invalid, and you are no longer able to run secure transactions on your website. The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date.

Diagnostic Information:
Generating a Certificate Report

To generate a certificate report:

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.
2. Select the certificate for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold `Ctrl` as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

1. Recovery:

1. For details on DNS Configuration feature, see the DNS Configuration chapter in *Operation, Administration, and Maintenance (OAM) Guide*.
2. For details on Certificate Management feature, see the Certificate Management chapter in *Operation, Administration, and Maintenance (OAM) Guide*.
3. It is recommended to contact My Oracle Support if further assistance is needed.

10112 - Certificate Cannot be Used

Alarm Group:
AUD

Description:
The certificate cannot be used because the certificate is not available yet.

Severity:
Major

Instance:
<CertificateName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
certificateCannotBeUsed

Cause:
The certificate cannot be used because the certificate is not available yet.
Certificate Management
The Certificate Management feature allows users to configure certificates for:

- **HTTPS/SSL** - Allows secure login without encountering messages about untrusted sites
- **LDAP (TLS)** - Allows the LDAP server's public key to encrypt credentials sent to the LDAP server
- **TLS/DTLS over TCP/SCTP Transport** - Allows transport layer security protocols and encryption on a per connection basis at the application layer. For example, DSR local and peer node connections
- **Single Sign-On (SSO)** - Allows users to navigate among several applications without having to re-enter login credentials
- **Certificate Authority (CA)** - A digital certificate provided by a trusted source used to make secure connections between a client and server

> **Note:**
>
> When setting up Certificate Management, you must first assign a system domain name for the DNS configuration before importing any certificates.

If you allow a certificate to expire, the certificate becomes invalid, and you are no longer able to run secure transactions on your website. The Certification Authority (CA) prompts you to renew your SSL certificate before the expiration date.

Diagnostic Information:
Generating a Certificate Report

To generate a certificate report:

1. Click **Administration**, and then **Access Control**, and then **Certificate Management**.

2. Select the certificate for which you want to create a report.

> **Note:**
>
> To select multiple server groups, press and hold `Ctrl` as you click to select specific rows. Alternatively, if no servers are selected then all server groups appear in the report.

3. Click **Report**.
4. Click **Print** to print the report, or click **Save** to save a text file of the report.

Recovery:

1. For details on DNS Configuration feature, see the DNS Configuration chapter in *Operation, Administration, and Maintenance (OAM) Guide*.
2. For details on Certificate Management feature, see the Certificate Management chapter in *Operation, Administration, and Maintenance (OAM) Guide*.
3. It is recommended to contact My Oracle Support if further assistance is needed.

10115 - Health Check Started

Alarm Group:
LOG

Description:
Upgrade health check operation started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogHealthCheckStart

1. Recovery:

- No action required.

10116 - Health Check Successful

Alarm Group:
LOG

Description:
Upgrade health check operation completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogHealthCheckSuccess

1. Recovery:

- No action required.

10117 - Health Check Failed

Alarm Group:
LOG

Description:
Upgrade health check operation failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogHealthCheckFailed

1. Recovery:

- No action required.

10118 - Health Check Not Run

Alarm Type:
LOG

Description:
Upgrade health check not run.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogHealthCheckNotRun

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

10120 - Server Group Upgrade Started

Alarm Group:
LOG

Description:
The server group upgrade operation has started.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogSgUpgradeStart

1. Recovery:

- No action required.

10121 - Server Group Upgrade Cancelled - Validation Failed

Alarm Group:
LOG

Description:
The server group upgrade operation has been cancelled due to validation failure.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogSgUpgradeCancelled

1. Recovery:

- No action required.

10122 - Server Group Upgrade Successful

Alarm Group Group:
LOG

Description:
The server group upgrade operation completed successfully.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogSgUpgradeSuccess

1. Recovery:

- No action required.

10123 - Server Group Upgrade Failed

Alarm Group:
LOG

Description:
The server group upgrade operation failed.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogSgUpgradeFailed

1. Recovery:

- No action required. Alarm 10134 - Server Upgrade Failed is raised for each server in the server group that failed to upgrade. The alarm clears when the server upgrades successfully.

10124 - Server Group Upgrade Cancelled - User Request

Alarm Group:
LOG

Description:
The user cancelled the server group upgrade operation.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogSgUpgradeCancelledUser

1. Recovery:

- No action required.

10125 - Server Group Upgrade Failed

Alarm Group:
LOG

Description:
Server group upgrade operation failed.

Severity:
Major

Instance:
<ServerGroupName>

HA Score:
Normal

Auto Clear Seconds
0 (zero)

OID:
tekelecLogSgUpgradeFailAlm

Recovery

- It is recommended to contact My Oracle Support if further assistance is needed.

10130 - Server Upgrade Started

Alarm Group:
LOG

Description:
The server upgrade operation has started.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogServerUpgradeStart

1. Recovery:

- No action required.

10131 - Server Upgrade Cancelled

Alarm Group:
LOG

Description:
The server upgrade operation has been cancelled due to validation failure.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogServerUpgradeCancelled

1. Recovery:

- No action required.

10132 - Server Upgrade Successful

Alarm Group:
LOG

Description:
The server upgrade operation completed successfully.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogServerUpgradeSuccess

1. Recovery:

- No action required.

10133 - Server Upgrade Failed

Alarm Group:
LOG

Description:
The server upgrade operation failed.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogServerUpgradeFailed

1. Recovery:

- No action required. Alarm 10134 - Server Upgrade Failed is raised for each server that failed to upgrade. The alarm clears when the server upgrades successfully.

10134 - Server Upgrade Failed

Alarm Group:
LOG

Description:
The server upgrade operation failed.

Severity:
Major

Instance:
<HostName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tekelecLogServerUpgradeFailAlm

1. Recovery:

1. If a server upgrade fails, this alarm clears when the server upgrades successfully. Upgrade the server individually or as part of a server group or site upgrade.
   If more than one server in the same server group or site fails to upgrade, the server group and site upgrades may be useful because both methods will attempt to upgrade all of the failed servers within the server group or site, respectively. Upgrading all servers in a server group is useful if the server group has multiple upgrade failures. Upgrading all servers in a site is useful if servers in multiple server groups contained in a site have upgrade failures.

2. To upgrade individual servers:
   a. Navigate to the Upgrade page (**Administration**, and then **Software Management**, and then **Upgrade**).
   b. To upgrade a NOAM server, select the NOAM tab and proceed to 2.e.
   c. To upgrade a server that is not a NOAM server, select the SOAM site tab associated with the server(s) that raised the alarm.
   d. Select the sub-tab associated with the server group containing the server(s) that raised the alarm.
   e. Select the individual server(s) and then click the **Upgrade Server** button to start the upgrade on the selected servers.

   > **Note:**
   >
   > Servers cannot be selected across tabs. If there are servers in multiple server groups, you must restart the server upgrade for each additional Server Group tab, or perform a server group or site upgrade.

3. To upgrade all servers in a server group:
   a. Navigate to the Upgrade page (**Administration**, and then **Software Management**, and then **Upgrade**).
   b. To upgrade a NOAM server, select the NOAM tab and proceed to 3.e.
   c. To upgrade a server that is not a NOAM server, select the SOAM site tab associated with the server(s) that raised the alarm.
   d. Select the sub-tab associated with the server group containing the server(s) that raised the alarm.
   e. Click **Auto Upgrade** to upgrade all servers in the server group. (Do not select any servers.)

   > **Note:**
   >
   > The active server in the NO server group never upgrades automatically.

   An alternative method to upgrade a server group that is not a NOAM server group is to upgrade selected server groups from the Entire Site sub-tab. The site upgrade form does not offer as many options as the automated server group upgrade.

   To upgrade all servers in a server group using the alternative method:

   a. Navigate to the Upgrade page (**Administration**, and then **Software Management**, and then **Upgrade**).
   b. Select the SOAM site tab associated with the server(s) that raised the alarm. Remain on the Entire Site sub-tab.

> **Note:**
>
> The Entire Site sub-tab only appears when the site contains more than one server group.

c. Select the individual server group(s) then click the **Upgrade Server Group** button to start the upgrade on the selected server group(s).

4. To upgrade entire sites:

   a. Navigate to the Upgrade page (**Administration**, and then **Software Management**, and then **Upgrade**).

   b. Select the SOAM site tab associated with the server(s) that raised the alarm. Remain on the Entire Site sub-tab.

> **Note:**
>
> The Entire Site sub-tab only appears when the site contains more than one server group.

   c. Click **Site Upgrade** to upgrade all server groups in the site. (Do not select any server groups.)

10140 - Site Upgrade Started

Alarm Group:
LOG

Description:
Site upgrade operation started.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogSiteUpgradeStart

1. Recovery:

- No action required.

10141 - Site Upgrade Cancelled

Alarm Group:
LOG

Description:
Site upgrade cancelled - validation failed.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogSiteUpgradeCancelled

1. Recovery:

- No action required.

10142 - Site Upgrade Successful

Alarm Group:
LOG

Description:
Site upgrade operation completed successfully.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogSiteUpgradeSuccess

1. Recovery:

- No action required.

10143 - Site Upgrade Failed

Alarm Group:
LOG

Description:
Site upgrade operation failed.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogSiteUpgradeFailed

1. Recovery:

- No action required. Alarm 10134 - Server Upgrade Failed is raised for each server in the site that failed to upgrade. The alarm clears when the server upgrades successfully.

10144 - Site Upgrade Cancelled - User Request

Alarm Group:
LOG

Description:
Site upgrade cancelled by user.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
tekelecLogSiteUpgradeCancelledUser

1. Recovery:

- No action required.

10145 - Site Upgrade Failed

Alarm Group:
LOG

Description:
Site upgrade operation failed.

Severity:
Major

Instance:
<SiteName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tekelecLogSiteUpgradeFailed

1. Recovery:

- No action required. Alarm 10134 - Server Upgrade Failed is raised for each server in the site that failed to upgrade. The alarm clears when the server upgrades successfully.

10151 - Login Successful

Alarm Group:
LOG

Description:
The login operation was successful.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLoginSuccessNotify

1. Recovery:

- No action required.

10152 - Login Failed

Alarm Group:
LOG

Description:
The login operation failed

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLoginFailedNotify

1. Recovery:

- Verify login information and case is correct, and re-enter.

10153 - Logout Successful

Alarm Group:
LOG

Description:
The logout operation was successful.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecLogoutSuccessNotify

1. Recovery:

- No action required.

10154 - User Account Disabled

Alarm Group:
AUTH

Description:
User account has been disabled due to multiple login failures.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
tekelecAccountDisabledNotify

1. Recovery:

- The alarm clears if the account is automatically re-enabled. Otherwise, the administrator must enable or delete user account.

10155 - SAML Login Successful

Alarm Group:
LOG

Description:
SAML login successful.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecSamlLoginSuccessNotify

1. Recovery:

- This is not a failure alarm. It is an indication the user was successfully authenticated for login to the GUI. This applies to both conventional login and Single Sign On (SSO) login.

10156 - SAML Login Failed

Alarm Group:
LOG

Description:
An attempt to log into the GUI via conventional login or via SSO login failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
1

OID:
tekelecSamlLoginFailed

1. Recovery:

1. Use correct username and password to log in.
2. For failed SSO login, verify SSO was properly configured. Collect logs and it is recommended to contact My Oracle Support if the problem persists.

10200 - Remote Database Reinitialization in Progress

Alarm Group:
CFG

Description:
The remote database reinitialization is in progress. This alarm is raised on the active NOAM server for the server being added to the server group.

Severity:
Minor

Instance:
<hostname of remote server>

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
apwSgDbReinitNotify

1. Recovery:
1. Check to see that the remote server is configured.
2. Make sure the remote server is responding to network connections.
3. If this does not clear the alarm, delete this server from the server group.
4. It is recommended to contact My Oracle Support if further assistance is needed.

10300 - SNMP Trapping Not Configured

Alarm Group:
DB

Description:
SNMP trapping not configured for site.

SeverityL
Minor

Instance:
<Hostname>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
apwSnmpTrappingNotConfiguredForSite

1. Recovery:

- The SNMP trap configuration is in SITE mode. Configure SNMP for the site <Hostname> belongs to.

IDIH (11500-11549)

This section provides information and recovery procedures for **IDIH** alarms, which range from 11500 to 11549.

11500 - Tracing Suspended

Alarm Group:
IDIH

Description:
IDIH trace has been suspended due to DA-MP (danger of) CPU congestion.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterTracingSuspendedAlarmNotify

1. Recovery:

- No action required. Tracing will resume once the danger of CPU congestion subsides.

11501 - Trace Throttling Active

Alarm Group:
IDIH

Description:
Troubleshooting trace has been throttled on some DA-MPs due to IDIH TTR bandwidth usage exceeding provisioned limit.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterTracingThrottledAlarmNotify

1. Recovery:

- No action required

11502 - Troubleshooting Trace Started

Alarm Group:
IDIH

Description:
A troubleshooting trace instance was started.

Severity:
Info

Instance:
<TraceInstanceId>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIDIHTraceStartedNotify

1. Recovery:

- No action required.

11503 - Troubleshooting Trace Stopped

Alarm Group:
IDIH

Description:
A troubleshooting trace instance was stopped.

Severity:
Info

Instance:
<TraceInstanceId>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIDIHTraceStoppedNotify

1. Recovery:

- No action required.

11506 - Invalid IDIH-Trace AVP

Alarm Group:
IDIH

Description:
An IDIH-Trace AVP has been received with an invalid format.

Severity:
Info

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
eagleXgDiameterInvalidIDIHTraceAvpNotify

1. Recovery:

1. If the message came from a peer that is not a DA-MP, verify the peer is not modifying the AVP value (peers may retain the IDIH-Trace AVP unchanged, or remove it entirely, at their discretion).
2. If the message came from a peer that is a DA-MP, it is recommended to contact My Oracle Support if further assistance is needed.

11507 - Unable to Run Network Trace at This Site

Alarm Group:
IDIH

Description:
A network trace could not be run at this site because the connection or peer referenced by the trace scope value is not configured at this site. The trace still runs at sites that have this entity configured.

Severity:
Info

Instance:
<TraceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterUnableToRunNetworkTraceAtThisSiteNotify

1. Recovery:

- No action required; the trace still runs at all sites that have the indicated object configured at their site.

11508 - Network Trace Configuration Error

Alarm Group:
IDIH

Description:
An error occurred during configuration of the network trace. Please delete the trace definition.

Severity:
Minor

Instance:
<TraceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterNetworkTraceConfigurationErrorNotify

1. Recovery:

- Delete the network trace that raised the alarm.

11509 - Site Trace Configuration Error

Alarm Group:
IDIH

Description:
An error occurred during configuration of the site trace. Please delete the trace definition.

Severity:
Minor

Instance:
<TraceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterSiteTraceConfigurationErrorNotify

1. Recovery:

- Delete the site trace that raised the alarm.

11510 - Network Trace Activation Error

Alarm Group:
IDIH

Description:
Network trace is not active on this site. A temporary error occurred during the activation of the network trace.

Severity:
Minor

Instance:
<TraceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterNetworkTraceActivationErrorNotify

1. Recovery:

- No action required.

11511 - Invalid DIH HostName

Alarm Group:
DIAM

Description:
Unable to connect via ComAgent to remote DIH server with hostname.

Severity:
Minor

Instance:
String of Configured DIH HostName

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterInvalidDihHostNameAlarmNotify

1. Recovery:

- No action required.

SDS (14000-14999)

This section provides information and recovery procedures for **SDS** alarms and events, ranging from 14000-14999.

14100 - Interface Disabled

Alarm Group:
PROV

Description:
Provisioning interface is manually disabled.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not automaticall clear after a set time

OID:
sdsProvInterfaceDisabled

1. Recovery:

1. xxx

2. Enable the interface to clear the alarm.

14101 - No Remote Connections

Alarm Group:
PROV

Description:
No remote provisioning clients are connected.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not automatically clear.

OID:
sdsProvNoRemoteConnections

1. Recovery:

- The alarm will clear when at least one remote provisioning client is connected.

14102 - Connection Failed

Alarm Group:
PROV

Description:
Provisioning client connection initialization failed due to an error specified in additional information. See trace log for details. (CID=<Connection ID>, IP=<IP Address>).

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
300

OID:
sdsProvConnectionFailed

1. Recovery:

- Alarm automatically clears after 5 minutes or when connected.

14103 - Both Port Identical

Alarm Group:
PROV

Description:
Both XML and SOAP provisioning client connection are disables since same port is configured for both.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvBothPortIdentical

1. Recovery:

- Alarm clears when one of the ports is changed.

14120 - Connection Established

Alarm Group:
PROV

Description:
Provisioning client connection established.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvConnectionEstablished

1. Recovery:

- No action required for this alarm.

14121 - Connection Terminated

Alarm Group:
PROV

Description:
Provisioning client connection terminated due to the error specified in additional information.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvConnectionTerminated

1. Recovery:

- No action required for this alarm.

14122 - Connection Denied

Alarm Group:
PROV

Description:
Provisioning client connection denied due to the error specified in additional information.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvConnectionDenied

1. Recovery:

- No action required for this alarm.

14140 - Import Throttled

Alarm Group:
PROV

Description:
Provisioning import throttled to prevent overrunning database service processes.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
5

OID:
sdsProvImportThrottled

1. Recovery:

- Alarm automatically cleared in 5 seconds after throttling subsides.

14150 - Import Initialization Failed

Alarm Group:
PROV

Description:
Provisioning import failed due to the initialization error specified in additional information. See trace log for details.

Severity:
Major

Instance:
provimport

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvImportInitializationFailed

1. Recovery:

- Alarm clears when initialization completes successfully.

14151 - Import Generation Failed

Alarm Group;
PROV

Description:
Provisioning import failed due to the import file execution error specified in the additional information. See the trace log for details.

Severity:
Major

Instance:
provimport

HA Score:
Normal

Auto Clear Seconds:
12 hours

OID:
sdsProvImportGenerationFailed

1. Recovery:

- Alarm clears automatically after 12 hours or when initialization completes successfully.

14152 - Import Transfer Failed

Alarm Group:
PROV

Description:
Provisioning import operation failed due to the file transfer error specified in additional information. See trace log for details.

Severity:
Major

Instance:
provimport

HA Score:
Normal

Auto Clear Seconds:
12 hours

OID:
sdsProvImportTransferFailed

1. Recovery:

- Alarm clears automatically after 12 hours or when the file transfer completes successfully.

14153 - Export Initialization Failed

Alarm Group:
PROV

Description:
Provisioning export failed due to the initialization error specified in the additional information. See trace log for details.

Severity:
Major

Instance:
provexport

HA Score:
Normal

Auto Clear Seconds:
12 hours

OID:
sdsProvExportInitializationFailed

1. Recovery:

- Alarm clears automatically after 12 hours or when initialization completes successfully.

14154 - Export Generation Failed

Alarm Group:
PROV

Description:
Provisioning export operation failed due to the export file generation error specified in the additional information. See trace log for details.

Severity:
Major

Instance:
provexport

HA Score:
Normal

Auto Clear Seconds:
12 hours

OID:
sdsProvExportGenerationFailed

1. Recovery:

- Correct the problem and try the export again.

14155 - Export Transfer Failed

Alarm Group:
PROV

Description:
Provisioning export operation failed due to the file transfer error specified in the additional information. See trace log for details.

Severity:
Major

Instance:
provexport

HA Score:
Normal

Auto Clear Seconds:
12 hours

OID:
sdsProvExportTransferFailed

1. Recovery:

- Correct the problem and try the export again.

14160 - Import Operation Completed

Alarm Group:
PROV

Description:
All files were imported successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvImportOperationCompleted

1. Recovery:

- No action required for this alarm.

14161 - Export Operation Completed

Alarm Group:
PROV

Description:
All scheduled exports completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvExportOperationCompleted

1. Recovery:

- No action required for this alarm.

14170 - Remote Audit Started and In Progress

Alarm Group:
PROV

Description:
Remote Audit started and is in progress.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvRemoteAuditStartedAndInProgressNotify

1. Recovery:

- No action required for this alarm.

14171 - Remote Audit Aborted

Alarm Group:
PROV

Description:
Remote audit aborted.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvRemoteAuditAbortedNotify

1. Recovery:

- No action required for this alarm.

14172 - Remote Audit Failed to Complete

Alarm Group:
PROV

Description:
Remote audit failed to complete.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvRemoteAuditFailedToCompleteNotify

1. Recovery:

- No action required for this alarm.

14173 - Remote Audit Completed

Alarm Group:
PROV

Description:
Remote Audit completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvRemoteAuditCompletedNotify

1. Recovery:

- No action required for this alarm.

14174 - NPA Split Pending Request Deleted

Alarm Group:
PROV

Description:
A pending NPA split has been deleted by the user before it could become active on its start date.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvNpaSplitPendingRequestDeleted

1. Recovery:

- No action required for this alarm.

14175 - NPA Split Activation Failed

Alarm Group:
PROV

Description:
NPA Split activation failed. See trace log for details.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvNpaSplitActivationFailed

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

14176 - NPA Split Started and Is Active

Alarm Group:
PROV

Description:
NPA Split started and is active.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvNpaSplitActivated

1. Recovery:

- No action required for this alarm.

14177 - NPA Split Completion Failed

Alarm Group:
PROV

Description:
NPA split completion failed. See trace log for details.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvNpaSplitCompletionFailed

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

14178 - NPA Split Completed

Alarm Group:
PROV

Description:
NPA split completed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsProvNpaSplitCompleted

1. Recovery:

- No action required for this alarm.

14179 - MSISDN Deleted From Blacklist

Alarm Group:
PROV

Description:
Previously blacklisted MSISDN is now a routing entity.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sdsProvMsisdnDeletedFromBlacklist

1. Recovery:

- No action necessary.

14180 - IMSI Deleted from Blacklist

Alarm Group:
PROV

Description:
Previously Blacklisted IMSI is now a Routing Entity

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sdsProvImsiDeletedFromBlacklist

1. Recovery:

- No action necessary.

14188 - PdbRelay Not Connected

Alarm Group:
PROV

Description:
PdbRelay not connected.

- The SDS Command Log does not go back far enough to resume relaying commands. A bulk load of HLRR is required.
- Neither Primary nor Disaster Recovery Virtual IP address is configured for the HLRR.
- The connection is failing with the error shown in Additional Info.

Severity:
Major

Instance:
pdbrelay

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sdsProvRelayNotConnectedNotify

1. Recovery:

1. Perform Bulk Load Procedure at the HLRR.
2. Configure the HLRR address in the SDS GUI.
3. Verify network connectivity with the HLRR.

14189 - PdbRelay Time Lag

Alarm Group:
PROV

Description:
Pdbrelay feature is enabled but is falling behind. The time between timestamps of the last record processed and the latest entry in the Command Log has exceeded time limit threshold.

- Critical: 27 minutes
- Major - 12 minutes
- Minor - 3 minutes

Severity:
Critical, Major, Minor

Instance:
pdbrelay

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sdsProvRelayTimeLagNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

14198 - ProvDbException

Alarm Group:
PROV

Description:
The rate of ProvDbException errors has exceed the threshold.

- Critical: 1000 errors per second
- Major: 100 errors per second
- Minor: Any occurrence

Severity:
Critical, Major, Minor

Instance:
ProvDbException, SDS

HA Score:
Normal

Auto Clear Seconds:
3600

OID:
sdsProvDbExceptionNotify

1. Recovery:

- No action required.

14200 - DP Stack Event Queue Utilization

Alarm Group:
DPS

Description:
The percent utilization of the DP Stack Event Queue is approaching its maximum capacity.

Severity:

- Minor when utilization exceeds 60%.
- Major when utilization exceeds 80%.
- Critical when utilization exceeds 95%.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsDpsStackEventQueueUtilizationNotify

1. Recovery:

- Minor alarm clears when utilization falls below 50%.
- Major alarm clears when utilization falls below 70%.
- Critical alarm clears when utilization falls below 90%.

14301- ERA Responder Failed

Alarm Group:
ERA

Description:
Event responder failed due to an internal error.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
sdsEraResponderFailed

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

SS7/Sigtran (19200-19299)

This section provides information and recovery procedures for SS7/Sigtran alarms ranging from 19200 - 19299.

19200 - RSP/Destination Unavailable

Alarm Group:
SS7

Description:
Unable to access the SS7 Destination Point Code because the Remote Signaling Point status is unavailable.

Severity:
Critical

Instance:
RSP Name

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlRspUnavailableNotify

1. Recovery:
1. RSP/Destination status can be monitored from the SOAM GUI by navigating to **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
   - If the RSP/Destination becomes unavailable due to a link set failure, the MP server automatically attempts to recover all links not manually disabled.
   - If the RSP/Destination becomes unavailable due to the receipt of a TFP, the route's status is periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Navigate to **SS7/Sigtran**, and then **Maintenance**, and then **Link Sets** to check the status of linkset links to the adjacent server.
3. Navigate to **Transport Manager**, and then **Maintenance**, and then **Transport** to check the SCTP status to the adjacent server.
4. Verify IP network connectivity exists between the MP server and the adjacent servers.
5. If all the connections to adjacent server are OK, then check the connections between adjacent server and Remote Signaling Point. The specific steps depend on the adjacent server type.
6. Check the event history logs for additional SS7 events or alarms from this MP server.
7. Verify the adjacent server is not under maintenance.
8. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19201 - RSP/Destination Route Unavailable

Alarm Group:
SS7

Description:
Unable to access the SS7 Destination point code via this route.

Severity:
Minor

Instance:
<Route Name>

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlRouteUnavailableNotify

1. Recovery:

1. Route status can be monitored from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
   - If the route becomes Unavailable due to a link set failure, the MP server will attempt to automatically recover all links not manually disabled.
   - If the route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify the adjacent server is not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19202 - Linkset Unavailable

Alarm Group:
SS7

Description:
The SS7 link set to an adjacent signaling point has failed.

Severity:
Major

Instance:
<LinkSetName>

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlLinksetUnavailableNotify

1. Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link set status can be monitored from **SS7/Sigtran**, and then **Maintenance**, and then **Linksets**.
3. Verify IP network connectivity exists between the MP server and the adjacent servers.

4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify the adjacent server is not under maintenance.
6. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19203 - Link Unavailable

Alarm Group:
SS7

Description:
M3UA has reported to M3RL that a link is out of service.

Severity:
Minor

Instance:
<Link Name>

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlLinkUnavailableNotify

1. Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link status can be monitored from **SS7/Sigtran**, and then **Maintenance**, and then **Links**.
3. Verify IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify the adjacent server is not under maintenance.
6. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19204 - Preferred Route Unavailable

Alarm Group:
SS7

Description:
M3RL has started to use a lower priority (higher cost) route to route traffic toward a given destination address, because the higher priority (lower cost) route specified for that RSP/Destination has become Unavailable.

Severity:
Major

Instance:
RSP Name

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlPreferredRouteUnavailableNotify

1. Recovery:

1. If the preferred route becomes Unavailable due to the receipt of a TFP, the route's status will be periodically audited by sending RST messages to the adjacent point code which sent the TFP.
2. Route status can be monitored from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
3. Verify IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs for additional SS7 events or alarms from this MP server.
5. Verify the adjacent server is not under maintenance.
6. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19205 - TFP Received

Alarm Gorup:
SS7

Description:
The TFP message was received by M3RI layer; an adjacent point code has reported it no longer has any available routes to the RSP/Destination.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7M3rlTfpReceivedNotify

1. Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
2. Follow local procedures to determine the reason why the PC was prohibited.

19206 - TFA Received

Alarm Group:
SS7

Description:
TFA message received by M3RL layer; an adjacent point code has reported it has an available route to the RSP/Destination.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7M3rlTfaReceivedNotify

1. Recovery:

- Monitor the RSP/Destination status from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.

19207 - TFR Received

Alarm Group:
SS7

Description:
TFR message received by M3RL layer; an adjacent point code has reported an available route to the RSP/Destination has a restriction/limitation.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7M3rlTfrReceivedNotify

1. Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
2. Follow local procedures to determine the reason why the PC was prohibited.

19208 - TFC Received

Alarm Group:
SS7

Description:
TFC message received by M3RL layer; an adjacent or non-adjacent point code is reporting the congestion level of a RSP/Destination.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7M3rlTfcReceivedNotify

1. Recovery:

1. RSP/Destination status can be monitored from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
2. Follow local procedures to determine the reason why the PC was prohibited.

19209 - M3RL Routing Error

Alarm Group:
SS7

Description:
A message was discarded due to a routing error.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7M3rlRoutingFailureNotify

1. Recovery:

1. Each MP's assigned point code can be monitored from **SS7/Sigtran**, and then **Configuration**, and then **Local Signaling Points**.
2. If the event was caused by:
   - The DPC of an egress message is not configured as a remote signaling point, then look at the routing label in the event additional information, determine the DPC, and verify the DPC is configured as an RSP.
   - The DPC of an egress message is configured but not available for routing, then look at the routing label in the event additional information, determine the DPC, verify a route exists for the DPC, and use the RSP status screen to verify a route is available for the RSP.
   - The DPC of an ingress message does not match the TPC or CPC of the MP server group, then either signaling is being misdirected by the STP toward the MP, or the MP server's LSP is misconfigured. Look at the routing label in the event additional information for the OPC and DPC of the ingress message.
3. If a high number of these errors occurs, then an internal routing table problem might exist. It is recommended to contact My Oracle Support if further assistance is needed.

19210 - M3RL Routing Error - Invalid NI

Alarm Group:
SS7

Description:
The message was discarded due to a routing error. The NI (Network Indicator) value received in a message from the network is not assigned to the MP. This event is generated under the following circumstances:

- The NI in the MTP3 routing label of the ingress message is not supported for the given network signaling domain for a provisioned Local Signaling Point.
- For an ingress ANSI SCCP message, bit-8 in the SCCP CDPA address indicator octet indicates the CDPA is encoded as per international specifications:
  - A "0" in bit-8 indicates the address is international and both the address indicator and the address are coded according to international specifications.
  - A "1" in bit-8 indicates the address is national and both the address indicator and the address are coded according to national specifications.

    The NI cannot be International for ANSI messages, since the ordering of the subsystem number indicator field and the point code indicator fields are in the reverse order in the ITU specification.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7M3rlRoutingFailureInvalidNiNotify

1. Recovery:

1. The Signaling Transfer Point or Signaling Gateway routing tables may be inconsistent with the NI assigned to the MP. You can monitor each MP's assigned NI value from **SS7/Sigtran**, and then **Configuration**, and then **Remote Signaling Points**.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19211 - M3RL Routing Error - Invalid SI

Alarm Group:
SS7

Description:
The message was discarded due to a routing error. The SI value received in a message from the network is associated with a user part that is not currently supported.

Severity:
Info

Instance:
RSP Name

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7M3rlRoutingFailureInvalidSiNotify

1. Recovery:

1. If the SI received is not a **0** (SNM) or **3** (SCCP), verify the STP/SG and the point code that created the message have correct routing information.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19217 - Node Isolated - All Links Down

Alarm Group:
SS7

Description:
All configured links are down; either failed or disabled. No M3UA signaling is possible. The node is isolated from the network. All M3UA connectivity to the SS7/Sigtran network has either failed or has been manually disabled.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlNodeIsolatedAllLinkDownNotify

1. Recovery:

1. On the active SO, navigate to **SS7/Sigtran**, and then **Maintenance**, and then **Links** to check whether any of the links are manually disabled that should not be. If so, click **Enable** to enable the manually disabled links.
2. On the active SO, navigate to **Transport Manager**, and then **Maintenance**, and then **Transport** to verify the transports are enabled.
3. Go to the specific SS7MP and verify the IP address and NIC status.
4. On the specific SS7MP, verify the adjacent server IP address is available.
5. View the active alarms and event history logs by navigating to **Alarms & Events**, and then **View Active** and **Alarms & Events**, and then **View History**. Look for significant events that may affect the IP network, associations, or links.
6. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19226 - Timed Out Waiting for ASP-UP-ACK

Alarm Group:
SS7

Description:
When an association is in the **Enabled** administrative state, part of the association initialization involves sending an ASP-UP from the MP server and receiving an ASP-UP-ACK from the adjacent server. If ASP-UP is sent, but no ASP-UP-ACK is received within State Management ACK Timer milliseconds, this event is generated and the ASP-UP is attempted again. ASP-UP attempts will continue indefinitely until

the association administrative state is set to **Blocked** or **Disabled**, or the SCTP transport fails, or the ASP-UP-ACK is received.

Severity:
Info

Instance:
<AssocName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7TimedOutWaitingForAspUpAckNotify

1. Recovery:

1. Verify the adjacent server on the Signaling Gateway is not under maintenance.
2. Verify the timer value for State Management ACK Timer is not set too short to allow the adjacent server to respond with an ASP-UP-ACK. This should be rare if the network is not congested.
3. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19227 - Received Unsolicited ASP-DOWN-ACK

Alarm Group:
SS7

Description:
The adjacent server at the specified IP address and port has sent an ASP-DOWN-ACK, but not in response to an ASP-DOWN message from the MP server. Normally this indicates the far-end of the association is being taken down for maintenance. If the association administrative state is **Enabled**, the MP server automatically attempts to bring the association back to ASP-UP. This is done by sending an ASP-UP.
The MP server continues to send ASP-UP until an ASP-UP-ACK is received, the SCTP association comes down, or the association administrative state is changed to **Blocked** or **Disabled**.

Severity:
Info

Instance:
<AssocName>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7ReceivedUnsolicitedAspDownAckNotify

1. Recovery:

1. Verify the adjacent server on the Signaling Gateway is not under maintenance.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19229 - Timed Out Waiting for ASP-ACTIVE-ACK

Alarm Group:
SS7

Description:
No ASP-ACTIVE-ACK is received in response to an ASP-ACTIVE message on the link within State Management ACK Timer milliseconds.

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7TimedOutWaitingForAspActiveAckNotify

1. Recovery:

1. Verify the adjacent server on the Signaling Gateway is not under maintenance.
2. Verify the timer value for State Management ACK Timer is not set too short to allow the adjacent server to respond with an ASP-ACTIVE-ACK. This should be rare if the network is not congested.
3. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19230 - Received Unsolicited ASP-INACTIVE-ACK

Alarm Group:
SS7

Description:
An unsolicited ASP-INACTIVE-ACK is received on the link.

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7ReceivedUnsolicitedAspInactiveAckNotify

1. Recovery:

1. Verify the adjacent server on the Signaling Gateway is not under maintenance.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19231 - Received Invalid M3UA Message

Alarm Group:
SS7

Description:
The far-end has sent an invalid M3UA message to which the MP server has responded with an M3UA ERROR message.

Severity:
Info

Instance:
<LinkName> or <AssocName> Information about the type of error and the accompanying diagnostic data is included in the event additional information.

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7ReceivedInvalidM3uaMessageNotify

1. Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the malformed message.
   - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
   - Error code 0x03 indicates an unsupported M3UA message class.
   - Error code 0x04 indicates an unsupported M3UA message type.
   - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.

- Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
- Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
- Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
- Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
- Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.

2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19233 - Failed to Send Non-DATA Message

Alarm Group:
SS7

Description:
An attempt to send an M3UA non-DATA message has failed. Non-DATA messages include SSNM, ASPSM, ASPTM, and MGMT messages. The message has been discarded. Possible reasons for the failure include:

- The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing the MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
- The socket has closed just as the send was being processed.

Severity:
Info

Instance:
<LinkName> or <AssocName>

> **Note:**
>
> Information about the type of error and the accompanying diagnostic data is included in the event additional information.

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7FailedToSendNonDataMessageNotify

1. Recovery:

1. Select **Alarms & Events**, and then **View History** and check the event history logs for additional SS7 events or alarms from this MP server.
2. Verify the adjacent server on the Signaling Gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.
3. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19234 - Local Link Maintenance State Change

Alarm Group:
SS7

Description:
The link administrative state is manually changed from one administrative state to another.

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awpss7LocalLinkMaintenanceStateChangeNotify

1. Recovery:

1. No action required if this was an expected change due to some maintenance activity. Otherwise, security logs can be examined on the SOAM server to determine which user changed the administrative state.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19235 - Received M3UA Error

Alarm Group:
SS7

Description:
An M3UA ERROR message is received from the adjacent server.

Severity:
Info

Instance:
<LinkName> or <AssocName>

> **Note:**
>
> Information about the type of error and the accompanying diagnostic data is included in the event additional information.

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7ReceivedM3uaErrorNotify

1. Recovery:

1. Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the ERROR message.
   - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
   - Error code 0x03 indicates an unsupported M3UA message class.
   - Error code 0x04 indicates an unsupported M3UA message type.
   - Error code 0x05 indicates an unsupported M3UA traffic mode.
   - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
   - Error code 0x09 indicates an invalid SCTP stream identifier. A DATA message was sent on stream 0.
   - Error code 0x0D indicates the message was refused due to management blocking. An ASP Up or ASP Active message was received, but refused for management reasons.
   - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
   - Error code 0x12 indicates a parameter field error. Parameter is malformed (e.g., invalid length).
   - Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and "Protocol Error" are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
   - Error code 0x14 indicates the destination status is unknown. This message can be sent in response to a DAUD from the MP server if the SG cannot or does not wish to provide the destination status or congestion information.
   - Error Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.

- Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.

2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19240 - Remote SCCP Subsystem Prohibited

Alarm Group:
SS7

Description:
The status of remote SCCP subsystem has changed to **Prohibited**.

Severity:
Minor

Instance:
<RMU>

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7RemoteSccpSubsystemProhibitedNotify

1. Recovery:

1. You can monitor destination status from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points** and RMU/subsystem status from **SS7/Sigtran**, and then **Maintenance**, and then **Remote MTP3 Users**.

   - If the subsystem's status changed to **Prohibited** because SCMG received a SSP message, an audit of the status of the RMU via the SCCP subsystem status test (SST) procedure is performed.
   - If the subsystem's status changed to **Prohibited** because SCCP received a MTP-PAUSE indication from M3RL, then recovery actions of restoring the RSP/Destination status to **Available** will be invoked by M3RL.
   - If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS `cause=unequipped user` indication from M3RL, then no automatic recovery will be initiated. Only manual action at the remote node can correct a remote point code that has not been configured with SCCP.
   - If the subsystem's status changed to **Prohibited** because SCCP received a MTP STATUS `cause=unknown` or `inaccessible` indication from M3RL, then SCCP will automatically invoke subsystem status testing depending upon the network type:
     - ANSI: subsystem status testing of all RMUs associated with the point code.
     - ITU: subsystem status testing SCMG (`SSN=1`) associated with the point code.

2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Select **Alarms & Events**, and then **View History** and check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify the adjacent server is not under maintenance.
5. Follow local procedures to determine the reason why the far-end SSN is down. If it is not down, but it continues to be reported as down, it is recommended to contact My Oracle Support if further assistance is needed.

19241 - SCCP Malformed or Unsupported Message

Alarm Group:
SS7

Description:
SCCP discarded an ingress message because the Message Type is not currently supported. The following connectionless message types are supported: UDT, XUDT, UDTS, and XUDTS. The following SCMG Message Types are supported: SSA, SSP, and SST.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7SccpMsgTypeUnrecognizedNotify

1. Recovery:
1. Investigate:
   - If the originator of the message is misconfigured.
   - If the network is misconfigured, causing messages to be routed to the wrong RSP/Destination.
   - If the message type is currently unsupported.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19242 - SCCP Hop Counter Violation

Alarm Group:
SS7

Description:
SCCP discarded an ingress message because a Hop Counter violation was detected.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7SccpHopCounterViolationNotify

1. Recovery:

1. One of the following conditions causes this error:
   - The originator of the message is setting the initial value too low.
   - The message is being rerouted too many times by the STPs, possibly because of an STP routing misconfiguration that has caused message looping.
2. It is recommended to contact My Oracle Support if further assistance is needed.

19243 - SCCP Routing Failure

Alarm Group:
SS7

Description:
SCCP was unable to route or process a message during SCCP processing for reasons (other than a global title translation failure, detected SCCP loop) possibly requiring operator intervention.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7SccpRoutingFailureNotify

1. Recovery:

1. These failures are typically associated with invalid information received in the SCCP messages. Check for the following:

- A misconfiguration of the SCCP at the originating or terminating node
- Network routing misconfiguration at the STPs

2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19244 - SCCP Routing Failure Network Status

Alarm Group:
SS7

Description:
SCCP was unable to route or process a message during SCCP processing due to transient conditions such as RSP/destination failures and remote or local subsystem failures.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7SccpRoutingFailureNetworkStatusNotify

1. Recovery:
1. Monitor status on the GUI Main Menu as follows:
   - Destination status from **SS7/Sigtran**, and then **Maintenance**, and then **Remote Signaling Points**.
   - RMU/subsystem status from **SS7/Sigtran**, and then **Configuration**, and then **Remote MTP3 Users**.
   - Local subsystem status from **SS7/Sigtran**, and then **Maintenance**, and then **Local SCCP Users**.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional SS7 events or alarms from this MP server.
4. Verify the adjacent server is not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19245 - SCCP GTT Failure

Alarm Group:
SS7

Description:
SCCP Global Title Translation has failed to determine a destination for a PDU. SCCP is invoking the message return procedure.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7SccpGttFailureNotify

1. Recovery:
1. Global title translation has failed. For the cause of the failure, look at the SCCP return cause and the called party address information in the event additional information field. Look for the following items:
   - Missing global title translation data.
   - Incorrect called party address information in the ingress message.
   - Point code paused or congested.
   - Subsystem prohibited or congested.
2. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19246 - Local SCCP Subsystem Prohibited

Alarm Group:
SS7

Description:
The status of the local SCCP subsystem has changed to **Prohibited**. This alarm is raised for one of the following conditions:

- When a new local SSN is configured and is in the disabled state.
- When a GUI maintenance operation is performed to disable the state of the local SSN.·
- On a system restart where the local SSN was is disabled state prior to the system restart.

Severity:
Major

Instance:
<LSP>, <SSN>

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7SCCPLocalSubsystemProhibitedNotify

1. Recovery:

- To clear the alarm:
  1. On the SOAM GUI, select **SS7/Sigtran**, and then **Configuration**, and then **Local SCCP Users**.
  2. Set the **Auto Refresh** for the page (upper right corner) to 15 so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.
  3. Click **Enable** to put the appropriate local SSN in the enabled state.

     A confirmation message appears.
  4. Click **OK**.

     The **Enable** link will be grayed out once the SSN transitions to the enabled state.

19248 - SCCP Segmentation Failure

Alarm Group:
SS7

Description:
SCCP Segmentation Procedure Failure

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7SccpSegmentationFailureNotify

1. Recovery:

1. This condition indicates segmentation procedure failure at the SCCP layer:
   - User data exceeds maximum size
   - Internal Error
2. Check the SCCP options configuration and maximum size limitations for the SS7 network.
3. It is recommended to contact My Oracle Support if further assistance is needed.

19249 - SCCP Reassembly Failure

Alarm Group:
SS7

Description:
SCCP Reassembly Procedure Failure

Severity:
Info

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7SccpReassemblyFailureNotify

1. Recovery:
1. This condition indicates reassembly procedure failure at the SCCP layer:
   - Reassembly time expired
   - Out of sequence segments
   - Internal error
2. Determine if the problem is a result of routing decision errors or latency from the SS7 network.
3. It is recommended to contact My Oracle Support if further assistance is needed.

19250 - SS7 Process CPU Utilization

Alarm Group:
SS7

Description:
The SS7 process, which is responsible for handling all SS7 traffic, is approaching or exceeding its engineered traffic handling capacity.

Severity:
Minor, Major, or Critical as shown in the GUI under **Alarms & Events**, and then **View Active.**

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7Ss7ProcessCpuUtilizationNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from **Status & Manage**, and then **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. The SS7 process may be experiencing problems. You monitor the alarm log from **Alarms & Events**, and then **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19251 - Ingress Message Rate

Alarm Group:
SS7

Description:
The ingress message rate (messages per second) for the MP is approaching or exceeding its engineered traffic handling capacity.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7IngressMsgRateNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from **Status & Manage**, and then **Server**
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19252 - PDU Buffer Pool Utilization

Alarm Group:
SS7

Description:
The percent utilization of the MP's PDU buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization, all new ingress messages will be discarded.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
<PoolName> Values: ANSI, ITUI, ITUN

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7PduBufferPoolUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can monitor MP server status from **Status & Manage**, and then **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from

Status & Manage, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being de-allocated to the pool when a PDU is successfully transmitted into the network. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log from **Alarms & Events**, and then **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19253 - SCCP Stack Event Queue Utilization

Alarm Group:
SS7

Description:
The percent utilization of the MP's SCCP stack event queue is approaching its maximum capacity.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7SccpStackEventQueueUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from **Status & Manage**, and then **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

4. If no additional congestion alarms are asserted, the SCCP Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log under **Alarms & Events**, and then **View Active**.
5. If the problem persists, It is recommended to contact My Oracle Support if further assistance is needed.

19254 - M3RL Stack Event Queue Utilization

Alarm Group:
SS7

Description:
The percent utilization of the MP's M3RL Stack Event Queue is approaching its maximum capacity.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlStackEventQueueUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from **Status & Manage**, and then **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3RL Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events**, and then **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19255 - M3RL Network Management Event Queue Utilization

Alarm Group:
SS7

Description:
The percent utilization of the MP's M3RL Network Management Event Queue is approaching its maximum capacity.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlNetMgmtEventQueueUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from **Status & Manage**, and then **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP under **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP under **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3RL Network Management Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events**, and then **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19256 - M3UA Stack Event Queue Utilization

Alarm Group:
SS7

Description:
The percent utilization of the MP's M3UA Stack Event Queue is approaching its maximum capacity.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3uaStackEventQueueUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from **Status & Manage**, and then **Server**.
2. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the M3UA Stack Event thread may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events**, and then **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19258 - SCTP Aggregate Egress Queue Utilization

Alarm Group:
SS7

Description:
The percent utilization of events queued to all SCTP associations on the MP server is approaching maximum capacity.

Severity:
Minor, Major, Critical as shown in the GUI under **Alarms & Events**, and then **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7SctpAggregateAssocWriteQueueUtilNotify

1. Recovery:

1. An IP network or STP/SG problem may exist preventing SCTP from transmitting messages into the network on multiple Associations at the same pace that messages are being received from the network.
2. One or more SCTP Association Writer threads may be experiencing a problem preventing it from processing events from its event queue. Examine the alarm log from **Alarms & Events**, and then **View Active**.
3. If one or more MPs in a server site have failed, the traffic will be distributed among the remaining MPs in the server site. You can view MP server status from **Status & Manage**, and then **Server**.
4. The misconfiguration of STP routing may result in too much traffic being distributed to the MP. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. Each MP in the server site should be receiving approximately the same ingress transaction per second.
5. There may be an insufficient number of MPs configured to handle the network traffic load. You can monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**. If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
6. If the problem persists, it is recommended to contact My Oracle Support if further assistance is needed.

19259 - Operation Discarded Due to Local Resource Limitation

Alarm Group:
SS7

Description:
Operation discarded due to local resource limitation.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapOpDiscardedLocalResLimitNotify

1. Recovery:

1. Determine if this condition indicates a software problem or unexpected TC User behavior.
2. It is recommended to contact My Oracle Support if further assistance is needed.

19260 - Transaction Could Not be Delivered to Remote TCAP Peer Due to Conditions in the Network

Alarm Group:
SS7

Description:
Transaction could not be delivered to remote TCAP peer due to conditions in the network.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapTransNotDeliveredToPeerNotify

1. Recovery:

1. This event indicates an SCCP service message (UDTS or XUDTS) was received from the network, meaning that the TCAP message could not be delivered to the remote TCAP peer. The event additional information field contains the first 80 octets of the SS7 message starting with the MTP3 routing label. This data can be used to determine the routing instructions for the message.
2. Verify the routing is configured correctly for the destination. If the routing configuration is correct, determine why the remote TCAP peer is not available.
3. It is recommended to contact My Oracle Support if further assistance is needed.

19262 - Operation Discarded Due to Malformed Component Received from Remote TCAP Peer

Alarm Group:
SS7

Description:
Operation discarded due to malformed component received from remote TCAP peer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapMalformedComponentFromRemoteNotify

1. Recovery:

1. This event indicates a TCAP component was received from the remote TCAP peer that could not be successfully decoded.
2. The event additional information field includes the reason why the decoding failed, plus the first 80 octets of the message starting with the MTP3 routing label. The message data can be used to determine the source of the malformed message.
3. It is recommended to contact My Oracle Support if further assistance is needed.

19263 - Transaction Discarded Due to Malformed Dialogue Message Received from Local TC User

Alarm Group:
SS7

Description:
Transaction discarded due to malformed dialogue message received from local TC user.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapMalformedDialogueFromLocalNotify

1. Recovery:

1. Determine if this condition indicates a software problem or unexpected TC user behavior.

2. It is recommended to contact My Oracle Support if further assistance is needed.

19264 - Transaction Discarded Due to Malformed Dialogue Message from Remote TCAP Peer

Alarm Group:
SS7

Description:
Transaction discarded due to malformed dialogue message received from local TC peer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapMalformedDialogueFromRemoteNotify

1. Recovery:

1. This event indicates a TCAP message was received from the remote TCAP peer that could not be successfully decoded.
2. The event additional information field includes the reason why the decoding failed, plus the first 80 octets of the message starting with the MTP3 routing label. The message data can be used to determine the source of the malformed message.
3. It is recommended to contact My Oracle Support if further assistance is needed.

19265 - Unexpected Event Received from Local TC User

Alarm Group:
SS7

Description:
Unexpected event received from local TC user.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapUnexpectedMsgFromLocalNotify

1. Recovery:

1. Determine if this condition indicates a software problem or unexpected TC user behavior.
2. The event additional information field includes a description of what event was received and why it was unexpected, as well as what was done with the operation or dialogue as a result.
3. It is recommended to contact My Oracle Support if further assistance is needed.

19266 - Unexpected Event Received from Remote TCAP Peer

Alarm Group:
SS7

Description:
Unexpected event received from remote TCAP peer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapUnexpectedMsgFromRemoteNotify

1. Recovery:

1. Determine if this condition indicates a software problem or unexpected TC peer behavior.
2. The event additional information field includes:
   - a description of what event was received and why it was unexpected
   - what was done with the operation or dialogue as a result
   - the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the malformed message.
4. It is recommended to contact My Oracle Support if further assistance is needed.

19267 - Dialogue Removed by Dialogue Cleanup Timer

Alarm Group:
SS7

Description:
Dialogue removed by dialogue cleanup timer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapDialogueRemovedTimerExpiryNotify

1. Recovery:

1. This event indicates a TCAP transaction containing no components was sent, but no response was received from the remote TCAP peer.
2. The event additional information field includes:
   - the local dialogue-id
   - the number of milliseconds that elapsed between the time the message was sent and the time that the message was discarded
   - the destination point code to which the message was destined
   - the SCCP called party address to which the message was destined
3. Check for SCCP events just before this event indicating a message could not be routed. If SCCP failed to route the message, verify a route exists for the destination to which the TCAP message was being sent.
4. If no SCCP routing failure event exists, investigate why the remote TCAP peer failed to respond. The DPC and called party address can be used to determine the destination to which the message was being sent.
5. It is recommended to contact My Oracle Support if further assistance is needed.

19268 - Operation Removed by Invocation Timer Expiry

Alarm Group:
SS7

Description:
Operation removed by invocation timer expiry.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapOperationRemovedTimerExpiryNotify

1. Recovery:

1. This event indicates a TCAP transaction containing no components was sent, but no response was received from the remote TCAP peer.
2. The event additional information field includes:
   - the local dialogue-id and invoke-id
   - the number of milliseconds that elapsed between the time the message was sent and the time that the operation was discarded
   - the destination point code to which the message was destined if the component was ever sent
   - the SCCP called party address to which the message was destined if the component was ever sent
3. Check for SCCP events just before this event indicating a message could not be routed. If SCCP failed to route the message, verify a route exists for the destination to which the TCAP message was being sent.
4. If no SCCP routing failure event exists, investigate why the remote TCAP peer failed to respond. The DPC and called party address (if present) can be used to determine the destination to which the message was being sent.
5. If the DPC and Called Party Address are not included in the additional information field, it indicates the component was created, but never sent.
6. It is recommended to contact My Oracle Support if further assistance is needed.

19269 - Dialogue Aborted by Remote TCAP Peer

Alarm Group:
SS7

Description:
Dialogue aborted by remote TCAP peer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapDialogueAbortByRemoteNotify

1. Recovery:

1. This event indicates a remote TCAP peer has aborted a dialogue.
2. The event additional information field includes:
   - the abort reason
   - the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the U-Abort or P-Abort message.
4. It is recommended to contact My Oracle Support if further assistance is needed.

19270 - Received Unsupported TCAP Message

Alarm Group:
SS7

Description:
Received unsupported TCAP message.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapUnsupportedTCAPMsgRcvdNotify

1. Recovery:

1. This event indicates an unsupported TCAP message has been received.
2. The event additional information field includes:
   - the abort reason
   - the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the unsupported message.
4. It is recommended to contact My Oracle Support if further assistance is needed.

19271 - Operation Rejected by Remote TCAP Peer

Alarm Group:
SS7

Description:
Operation rejected by remote TCAP peer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapReturnRejectByRemoteNotify

1. Recovery:
1. This event indicates a remote TCAP peer has rejected an operation.
2. The event additional information field includes:
   - the reject reason
   - the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the message.
4. It is recommended to contact My Oracle Support if further assistance is needed.

19272 - TCAP Active Dialogue Utilization

Alarm Group:
SS7

Description:
TCAP active dialogue utilization

Severity:
Minor, Major, Critical

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
0 (alarm does not autoclear)

OID:
awpss7TcapActiveDialogueUtilNotify

1. Recovery:

1. The percent utilization of the MP's dialogue table is approaching maximum capacity. This alarm indicates the number of active dialogues on the MP server is higher than expected.
2. If this problem persists and the dialogue table reaches 100% utilization, all new messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This condition may be caused by any of the following:
   - the incoming plus outgoing rate of new dialogues is higher than expected (possibly due to poor load balancing across MP servers, or too few MP servers to handle the load)
   - the duration of the dialogues is longer than expected
   - both the rate and duration are higher than expected
   - a software problem is preventing removal of completed dialogues
3. It is recommended to contact My Oracle Support if further assistance is needed.

19273 - TCAP Active Operation Utilization

Alarm Group:
SS7

Description:
TCAP active operation utilization

Severity:
Minor, Major, Critical

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
0 (alarm does not autoclear)

OID:
awpss7TcapActiveOperationUtilNotify

1. Recovery:

1. The percent utilization of the MP's component table is approaching maximum capacity. This alarm indicates the number of active egress TCAP operations on the MP server is higher than expected.
2. If this problem persists and the component table reaches 100% utilization, all new egress operations will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This may be caused by any of the following:
   - the outgoing rate of new operations is higher than expected (possibly due to a higher than expected average number of operations per message)

- the duration of the operations is longer than expected
- both the outgoing rate and duration are higher than expected
- a software problem is preventing removal of components

3. It is recommended to contact My Oracle Support if further assistance is needed.

19274 - TCAP Stack Event Queue Utilization

Alarm Group:
SS7

Description:
TCAP stack event queue utilization

Severity:
Minor, Major, Critical

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
0 (alarm does not autoclear)

OID:
awpss7TcapStackEventQueueUtilNotify

1. Recovery:

1. The percent utilization of the MP's TCAP Stack Event Queue is approaching its maximum capacity. This alarm indicates the number of ingress TCAP messages on the MP server is higher than expected.
2. If this problem persists and the queue reaches 100% utilization, all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted. This may be caused by any of the following:
   - the incoming rate of new TCAP messages is higher than expected (possibly due to poor load balancing across MP servers, or too few MP servers to handle the load)
   - a software problem is causing the messages to be processed more slowly than expected
3. It is recommended to contact My Oracle Support if further assistance is needed.

19275 - Return Error from Remote TCAP Peer

Alarm Group:
SS7

Description:
Return error from remote TCAP peer

Severity:
Info

Instance:
Application name

HA Score:
Normal

Auto Clear Seconds:
30

OID:
awpss7TcapReturnErrorFromRemoteNotify

1. Recovery:

1. This event indicates a remote TCAP peer has responded to an operation using Return Error.
2. The event additional information field includes:
   - the error reason
   - the first 80 octets of the message starting with the MTP3 routing label
3. The message data can be used to determine the source of the message.
4. It is recommended to contact My Oracle Support if further assistance is needed.

19276 - SCCP Egress Message Rate

Alarm Group:
SS7

Description:
The SCCP Egress Message Rate (Message per second) for the MP is approaching or exceeding its engineered traffic handling capacity.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (alarm does not autoclear)

OID:
awpss7SccpEgressMsgRateNotify

1. Recovery:

1. This condition indicates the SS7 Stack is reaching its engineered traffic handling capacity due to egress traffic received from application.
2. It is recommended to contact My Oracle Support if further assistance is needed.

19281 - TCAP Routing Failure

Alarm Group:
SS7

Description:
TCAP was unable to route message due to transient conditions such as destination failure or destination unavailability.

Severity:
Info

Instance:
Hostname

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awpss7TcapRoutingFailureNotify

1. Recovery:
1. This condition indicates failure at the TCAP layer due to XG SS7 node removal or congestion at Communication Agent.
2. It is recommended to contact My Oracle Support if further assistance is needed.

Transport Manager (19400-19419)

This section provides information and recovery procedures for Transport Manager alarms and events ranging from 19400-19419.

19400 - Transport Down

Alarm Group:
TMF

Description:
Transport Down

Severity:
Major

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrTransportDownNotify

1. Recovery:

1. The Active alarm instance data, which can be viewed from **Alarms & Events**, and then **View Active**, contains the Transport Name as configured in **Transport Manager**, and then **Configuration**, and then **Transport**

   Additional Information for the alarm can be found in **Alarms & Events**, and then **View Active or View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column. This column will include the local and remote IP addresses and ports, the administrative state, and the protocol state of the association.

   This alarm is raised when:

   - The association is configured and the admin state is enabled, but the SCTP transport is not in the ASP-UP protocol state for the M3UA plugin, or
   - The association is configured, but the SCTP transport is not in the APP-UP state for other plugins

   > **Note:**
   >
   > It is normal to have an association alarm if the association is in the Blocked or Disabled administrative state.

   This alarm is cleared when:

   - The association received an ASP-UP-ACK from the far-end and the SCTP transport in the ASP-UP state for the M3UA plugin, or
   - The SCTP transport is an APP-UP state for other plugins, or
   - The association is disabled/deleted

   If an association's protocol state does not match the association's administrative state, the system will automatically attempt to recover the association if configured as Initiator and enabled. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed association (default: 10 seconds).

   Association administrative states are set from **Transport Manager**, and then **Maintenance**, and then **Transport** by clicking on the desired action for the row containing the association. This screen is also used to monitor association status.

   To troubleshoot:

   - If the association is manually Blocked or Disabled, then no further action is necessary.
   - Verify the association's local IP address and port number are configured on the IP Signaling Gateway (Some Signaling Gateways only accept connections from IP addresses and ports they are configured to accept from).

- Verify the association's remote IP address and port correctly identify an SCTP listening port on the adjacent server.
- Verify IP network connectivity exists between the MP server and the adjacent server.
- Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
- Verify the adjacent server on the Signaling Gateway is not under maintenance.

2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19401 - Failed to Configure Transport

Alarm Group:
TMF

Description:
Failed to configure transport.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrFailedToConfigureTransportNotify

1. Recovery:

1. A Transport is configured each time the Transport attempts to connect or reconnect.
2. If transport configuration fails or the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19402 - Failed to Connect Transport

Alarm Group:
TMF

Description:
Failed to connect Transport

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
60

OID:
awptransmgrFailedToConnectTransportNotify

1. Recovery:

1. The Transport named in the Instance field has failed in a connection attempt. If configured as an SCTP Initiator, the system will automatically attempt to recover the association/connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If configured as an SCTP or UDP Listener, no further action is taken.

   To troubleshoot

   - Verify the transport's local IP address and port number are configured on the Adjacent Node (Some Nodes only accept connections from IP addresses and ports they are configured to accept connections from).
   - Verify the transport's remote IP address and port correctly identify an SCTP listening port on the adjacent node.
   - Verify IP network connectivity exists between the MP and the adjacent node.
   - Verify the timers in the transport's configuration set are not set too short to allow the connection to proceed. This should be rare if the IP network is functioning correctly.
   - Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
   - Verify adjacent server on the Signaling Gateway is not under maintenance.

2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19403 - Received Malformed SCTP Message (Invalid Length)

Alarm Group:
TMF

Description:
Received malformed SCTP message (invalid length).

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrReceivedMalformedTransSctpMessageNotify

1. Recovery:

1. An SCTP message was received containing a message not valid in length.
2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19404 - Far-End Closed the Transport

Alarm Group:
TMF

Description:
Far-end closed the transport.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awptransmgrFarEndClosedTheTransportNotify

1. Recovery:

1. The far-end of the SCTP association sent a SHUTDOWN or ABORT message to close the association. If an Initiator, the MP server automatically attempts to reestablish the connection. Connection attempts occur every "Connection Retry Interval" seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed association (default: 10 seconds). If a Listener, the MP server will only open the socket and await further messages from the far-end.

   To Troubleshoot:

   - Investigate the adjacent node at the specified IP address and port to determine if it failed or if it is under maintenance.
   - Check the adjacent node for alarms or logs that might indicate the cause for their closing the association.
2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19405 - Transport Closed Due to Lack of Response

Alarm Group:
TMF

Description:
Transport closed due to lack of response

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awptransmgrTransportClosedDueToLackOfResponseNotify

1. Recovery:

1. The adjacent node at the specified IP address and port failed to respond to attempts to deliver an SCTP DATA packet or SCTP heartbeat. If an SCTP Initiator, the transport is closed and the MP server automatically attempts to reestablish the connection. Connection attempts occur every **Connection Retry Interval** seconds, as defined in the Transport Configuration Set screen for the configuration set used by the failed transport (default: 10 seconds). If a Listener, the MP server will only open the socket and await further messages from the far-end.

   To troubleshoot:

   - Verify IP network connectivity still exists between the MP server and the adjacent server.
   - Verify the timers in the transport's configuration set are not set too short to allow the signaling to succeed. This should be rare if the IP network is functioning correctly.
   - Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
   - Verify the adjacent server on the Signaling Gateway is not under maintenance.

2. It is recommended to contact My Oracle Support if further assistance is needed.

19406 - Local Transport Maintenance State Change

Alarm Group:
TMF

Description:
Local transport maintenance state change.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrLocalTransportMaintenanceStateChangeNotify

1. Recovery:

1. No customer action is necessary if this was an expected change due to some maintenance activity. Otherwise, security logs can be examined on the NO/SO server to determine which user changed the administrative state.

   Transport status can be viewed using **Transport Manager**, and then **Maintenance**, and then **Transport**.

2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19407 - Failed to Send Transport DATA Message

Alarm Group:
TMF

Description:
Failed to send transport DATA message.

Severity:
Info

Instance:
<TransportName>, <TransportAdapter>, <TransportProtocol>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awptransmgrFailedToSendTransDataMessageNotify

1. Recovery:

1. An attempt to send an SS7 M3UA/ENUM DATA message has failed. The message has been discarded.

   For SCTP, Possible reasons for the failure include:

- The far-end is slow to acknowledge the SCTP packets sent by the MP server, causing the MP server's SCTP send buffer to fill up to the point where the message cannot be queued for sending.
- The socket has closed just as the send was being processed.

To Troubleshoot:

- Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
- Verify the adjacent server on the Signaling Gateway is not under congestion. The MP server will have alarms to indicate the congestion if this is the case.

2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19408 - Single Transport Egress-Queue Utilization

Alarm Group:
TMF

Description:
The percent utilization of the MP's single transport egress-queue is approaching its maximum capacity.

Severity:
Based on defined Thresholds. Minor, Major, Critical Engineered Max Value = 1000

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrTransSingleWriteQueueUtilNotify

1. Recovery:

1. The percent utilization of the MP's Transport Writer Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization, all new egress messages from the Transport will be discarded.

   This alarm should not normally occur when no other congestion alarms are asserted. This may occur for a variety of reasons:

   - An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being received form the network.
   - The SCTP Association Writer process may be experiencing a problem preventing it from processing events from its event queue. The alarm log should be examined from **Main Menu**, and then **Alarms & Events**.

- If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining Mps in the server site. MP server status can be monitored from **Status & Manage**, and then **Server Status**.
- The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
- There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from **Status & Manage**, and then **KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19409 - Message Rejected by ACL Filtering

Alarm Group:
TMF

Description:
The message is rejected based on configured Access Control List for transport.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
awptransmgrMessageRejectedByAclFilteringNotify

1. Recovery:
1. Verify the ENUM server's IP address is the ACL, or that the ACL is empty.
2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19410 - Adjacent Node IP Address State Change

Alarm Group:
TMF

Description:
State change of an IP address of a multi-homed adjacent node in SCTP transport.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrAdjIpAddrStateChangeNotify

1. Recovery:

1. Verify IP network connectivity still exists between the MP server and the adjacent server.
2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19411 - SCTP Transport Closed Due to Failure of Multi-Homing Validation

Alarm Group:
TMF

Description:
SCTP Transport closed due to failure of multi-homing validation.

Severity:
Info

Instance:
<TransportName>, <TransportId>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrSctpTransportRefusedNotify

1. Recovery:

1. Recheck the adjacent node's configure IP address and validation mode.
2. If alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19412 - SCTP Transport Configuration Mismatched for Adjacent Node IP

Alarm Group:
TMF

Description:
IP address advertised by an adjacent node in INIT/INIT-ACK chunk are different from configured IP addresses.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrSctpTransportCfgMismatchNotify

1. Recovery:

1. Recheck the configured IP address and transport configuration and validation mode.
2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

19413 - SCTP Transport Closed Due to Unsupported Peer Address Event Received

Alarm Group:
TMF

Description:
SCTP transport closed due to unsupported add/delete peer IP address event received in peer address notification.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrTransportClosedDueToUnsupportedEventNotify

1. Recovery:

1. Disable SCTP dynamic address reconfiguration at the adjacent node.
2. If the alarm persists, it is recommended to contact My Oracle Support if further assistance is needed.

Communication Agent, ComAgent (19420-19909)

This section provides information and recovery procedures for Communication Agent (ComAgent) alarms and events; and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the **Alarms & Events**, and then **View Active** GUI menu option. The alarms and events log can be viewed from the **Alarms & Events**, and then **View History** page.

19420 - BDFQFull - Broadcast Data Framework Work Queue Full

Alarm Group
SMS

Description
The BDF work queue depth size has reached full capacity.

Severity
Minor

Instance
N/A

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
cAFBDFQFullNotify

1. Recovery:

1. The system itself may be heavily loaded with work, causing this subsystem to also become overloaded. Check other system resources for signs of overload.
2. It is recommended to contact My Oracle Support for assistance if needed.

19421 - BDFThrotl - Broadcast Data Framework Throttle Traffic

Alarm Group
SMS

Description
The BDF subsystem is throttling traffic at sender.

Severity
Minor

Instance
N/A

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
cAFBDFThrotlNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

19422 - BDFInvalidPkt - Broadcast Data Framework Invalid Corrupt StackEvent

Alarm Group
SMS

Description
The BDF subsystem received a StackEvent that was somehow invalid, corrupt, or could not be delivered to the application.

Severity
Info

Instance
<Source IP>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
cAFBroadcastDataFrameworkInvalidStackEventNotify

1. Recovery:

1. If more messages of the same type occur, then check the site(s) and network for other possible corruption or overloaded conditions.
2. It is recommended to contact My Oracle Support for assistance if needed.

19800 - Communication Agent Connection Down

Alarm Group:
CAF

Description:
This alarm indicates that a Communication Agent is unable to establish transport connections with one or more other server, and this may indicate applications on the local server are unable to communicate with all of their peers. Generally this alarm is generated when a server or the IP network is undergoing maintenance or when a connection has been manually disabled.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFConnectionDownNotify

Cause:

- A connection becomes down. If a connection was already down, when another connection becomes down, then the count of connections is updated, and the alarm is re-asserted.
- A connection exits the down state, and there are other down connections. Update the connection count and re-assert the alarm.

Diagnostic Information:
This alarm indicates a Communication Agent is unable to establish transport connections with one or more other servers, and this may indicate applications on the local server are unable to communicate with all of their peers. Generally this alarm is asserted when a server or the IP network is undergoing maintenance or when a connection has been manually disabled.

Following problems could exist:

- The IP network may be experiencing problems due to which the heartbeat exchange between the peers are not successful.
- There are missing route information or incorrectly configured routes in **NOAM Configuration**, and then **Network**, and then **Routes**.

1. Recovery:

1. Navigate to **Alarms & Events**, and then **View History** to find additional information about the alarm.

   The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs by navigating to **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
3. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine which connections on the server have abnormal status.
4. If the connection is manually disabled, then no further action is necessary.
5. Verify the remote server is not under maintenance.
6. Verify IP network connectivity exists between the two connection end-points.
7. Verify the connection's local IP address and port number are configured on remote node.
8. Verify the Application Process using Communication Agent plug-in is running on both ends.
9. Verify the connection's remote IP address and port correctly identify remote's listening port.
10. It is recommended to contact My Oracle Support for assistance.

19801 - Communication Agent Connection Locally Blocked

Alarm Group:
CAF

Description:
This alarm indicates that one or more Communication Agent connections have been administratively blocked at the server asserting the alarm, and this is generally done as part of a maintenance procedure. A connection that is blocked cannot be used by applications to communicate with other servers, and so this alarm may indicate that applications are unable to communicate with their expected set of peers.

> **Note:**
>
> It is normal to have this alarm if the connection is in the Blocked administrative state on the near-side of the connection.

Severity:
Minor

Instance:
N/A

> **Note:**
>
> This alarm is cleared when:
>
> - Locally UNBLOCKed: An Admin Action to locally UNBLOCK the service connection and no other connection is locally blocked.
> - Deleted: The MP Server/Connection is deleted.
> - Failed: The Connection is terminated, due to Admin Disable action or Heartbeat failure or remote end initiated disconnection or any other reason.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFConnLocalBlockedNotify

1. Recovery:
1. Use **Alarms & Events**, and then **View History** to find additional information about the alarm.

   The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine which connections on the server have abnormal status.
4. If the expected set of connections is locally blocked, then no further action is necessary.
5. To remove a the local block condition for a connection, use the **Communication Agent**, and then **Maintenance**, and then **Connection Status** screen and click **Enable** for the desired connection.
6. It is recommended to contact My Oracle Support for assistance.

19802 - Communication Agent Connection Remotely Blocked

Alarm Group:
CAF

Description:
This alarm indicates that one or more Communication Agent connections have been administratively blocked at a remote server connected to the server, and this is generally done as part of a maintenance procedure. A connection that is blocked cannot be used by applications to communicate with other servers, and so this alarm

may indicate that applications are unable to communicate with their expected set of peers.

> **Note:**
>
> It is normal to have this alarm if the connection is in the Blocked administrative state on the far-side of the connection.

Severity:
Minor

Instance:
N/A

> **Note:**
>
> This alarm is cleared when:
>
> - Locally UNBLOCKed: An Admin Action to locally UNBLOCK the service connection and no other connection is locally blocked.
> - Deleted: The MP Server/Connection is deleted.
> - Failed: The Connection is terminated, due to Admin Disable action or Heartbeat failure or remote end initiated disconnection or any other reason.

HA Score:
Normal

Auto Clear Seconds:
0 (zero, no auto clear)

OID:
cAFConnRemoteBlockedNotify

1. Recovery:
1. Use **Alarms & Events**, and then **View History** to find additional information about the alarm.

   The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
3. Use **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine which connections on the server have abnormal status.
4. If the expected set of connections is locally blocked, then no further action is necessary.

5. To remove a the local block condition for a connection, use the **Communication Agent**, and then **Maintenance**, and then **Connection Status** screen and click **Enable** for the desired connection.
6. It is recommended to contact My Oracle Support for assistance.

19803 - Communication Agent Stack Event Queue Utilization

Alarm Group:
CAF

Description:
The percent utilization of the **Communication Agent** Task stack queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode.

Severity:
Minor, Major, Critical

Instance:
<ComAgent StackTask Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFQueueUtilNotify

Cause:
This alarm raises when KPI **ComAgentQueueUtil** exceeds the thresholds defined in the **SysMetricThreshold** table .

- MINOR: `ComAgentQueueUtil|CAF|-*|Current|19803|60|50|3000`
- MAJOR: `ComAgentQueueUtil|CAF|**|Current|19803|80|70|3000`
- CRITICAL: `ComAgentQueueUtil|CAF|*C|Current|19803|95|90|3000`

Diagnostic Information:
The percent utilization of the Communication Agent Task's Queue is approaching its defined capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded, based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode.
This alarm should not normally occur when no other congestion alarms are asserted. This may occur for a variety of reasons:

- An IP network or Adjacent node problem may exist preventing from transmitting messages into the network at the same pace that messages are being received from the network.

- The Task thread may be experiencing a problem preventing it from processing events from its event queue.
- The mis-configuration of Adjacent Node IP routing may result in too much traffic being distributed to the MP.
- There may be an insufficient number of MPs configured to handle the network traffic load.

1. Recovery:
1. Navigate to **Main Menu**, and then **Alarms & Events** to examine the alarm log.

   An IP network or Adjacent node problem may exist preventing from transmitting messages into the network at the same pace that messages are being received from the network. The Task thread may be experiencing a problem preventing it from processing events from its event queue. It is recommended to contact My Oracle Support for assistance.
2. Navigate to **Status & Manage**, and then **KPIs** to monitor the ingress traffic rate of each MP.

   Each MP in the server site should be receiving approximately the same ingress transaction per second.

   It is recommended to contact My Oracle Support for assistance.
3. If the MP ingress rate is approximately the same, there may be an insufficient number of MPs configured to handle the network traffic load.

   If all MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

   It is recommended to contact My Oracle Support for assistance.

19804 - Communication Agent configured connection waiting for remote client to establish connection

Alarm Group:
CAF

Description:
Communication Agent configured connection waiting for remote client to establish connection. This alarm indicates that a Communication Agent is waiting for one or more far-end client MPs to initiate transport connections. Generally this alarm is asserted when a client MP or the IP network is undergoing maintenance or when a connection has been manually disabled at a client MP.

> **Note:**
>
> It is normal to have this auto-clearing connection alarm for the remote server connections that configured manually in Client mode, but are not yet available for processing traffic.

Severity:
Minor

Instance:
N/A

> **Note:**
>
> The alarm is cleared when a server connection exits the forming state and no other connection having server connect mode is in the forming state or the auto-clear time-out occurs.
>
> - The MP Server/Connection is deleted
> - When connection is moved to TotallyBlocked/RemotelyBlocked/ InService state from Aligning
> - Auto Clear
> - Connection is disabled

HA Score:
Normal

Auto Clear Seconds:
300 (5 min)

OID:
cAFClientConnWaitNotify

1. Recovery:

1. Find additional information for the alarm in **Alarms & Events**, and then **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.

   The alarm is cleared only for remote server connections that are configured manually in “Client” mode. This mode is used to listen for connection requests from configured remote clients.

   - The MP Server/Connection is deleted
   - When connection is moved to TotallyBlocked/RemotelyBlocked/InService state from Aligning
   - Auto Clear
   - Connection is disabled
2. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
3. Check **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine which connections on the server have abnormal status.
4. Verify that the remote server is not under maintenance.
5. If the connection is manually disabled at the client MP, and it is expected to be disabled, then no further action is necessary.
6. If the connection has been manually disabled at the client MP, but it is not supposed to be disabled, then enable the connection by clicking on the 'Enable' action button on the Connection Status screen.

7. Verify that IP network connectivity exists between the two connection end-points.
8. Verify that the connection's local IP address and port number are configured on remote client MP.
9. Verify that the Application Process using Communication Agent plug-in is running on both ends.
10. Verify that the connection's remote IP address and port correctly identify remote's listening port.
11. It is recommended to contact My Oracle Support for assistance.

19805 - Communication Agent Failed To Align Connection

Alarm Group:
CAF

Description:
The Communication Agent failed to align connection. This alarm indicates that Communication Agent has established one or more transport connections with servers that are running incompatible versions of software, and so Communication Agent is unable to complete the alignment of the connection. A connection that fails alignment cannot be used by applications to communicate with other servers, and so this alarm may indicate that applications are unable to communicate with their expected set of peers.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFConnAlignFailedNotify

1. Recovery:
1. If the connection administrative action is set to ‘disable’, the alarm is cleared. No further action is necessary.
2. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
3. Find additional information for the alarm in **Alarms & Events**, and then **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
4. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
5. Check **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine which connections on the server have abnormal status.

For each connection reporting 'Aligning' connection status, determine the servers that are endpoints, and verify that the correct software is installed on each server. If incorrect software is present, then server maintenance may be required.

6. It is recommended to contact My Oracle Support for assistance.

19806 - Communication Agent CommMessage Mempool Utilization

Alarm Group:
CAF

Description:
The percent utilization of the **Communication Agent** internal resource pool (CommMessage) is approaching its defined capacity. If this problem persists and the usage reaches 100% utilization, **ComAgent** allocates the CommMessage objects from the heap. This should not impact the functionality, but may impact performance and/or latency.

Severity:
Critical, Major, Minor

Instance:
<ComAgent Process Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFPoolResUtilNotify

Cause:
This alarm raises when ComAgent mempool utilization exceeds threshold limits. Minor (>= 60%), Major (>=80%), Critical (>=95%), % level of Max = 65535.

Diagnostic Information:
The percent utilization of the Communication Agent internal resource pool, CommMessage is approaching its defined capacity. If this problem persists and the usage reaches 100% utilization, ComAgent will allocate the CommMessage objects from the heap. This should not impact the functionality, but may impact performance and/or latency.
This alarm usually occurs when other congestion alarms are asserted. This may occur for one of the following reasons:

- An IP network or adjacent node problem may exist preventing from transmitting messages into the network at the same pace that messages are being received from the network.
- The Task thread may be experiencing a problem preventing it from processing events from its internal resource queue.
- The mis-configuration of adjacent node IP routing may result in too much traffic being distributed to the MP.

- There may be an insufficient number of MPs configured to handle the network traffic load.

1. Recovery:

1. Navigate to **Alarms & Events** to examine the alarm log.

   An IP network or Adjacent node problem may exist preventing from transmitting messages into the network at the same pace that messages are being received from the network. The Task thread may be experiencing a problem preventing it from processing events from its internal resource queue. It is recommended to contact My Oracle Support for assistance.

2. Navigate to **Status & Manage**, and then **KPIs** to monitor the ingress traffic rate of each MP.

   Each **MP** in the server site should be receiving approximately the same ingress transaction per second.

   It is recommended to contact My Oracle Support for assistance.

3. If the **MP** ingress rate is approximately the same, there may be an insufficient number of MPs configured to handle the network traffic load.

   If all MPs are in a congestion state then the ingres rate to the server site is exceeding its capacity.

   It is recommended to contact My Oracle Support for assistance.

19807 - Communication Agent User Data FIFO Queue Utilization

Alarm Group:
CAF

Description:
The percent utilization of the Communication Agent User Data FIFO queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded, based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode.

Severity:
Minor, Major, Critical

Instance:
<ComAgent StackTask Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFUserDataFIFOUtilNotify

Cause:
Minor (>= 60%), Major (>=80%), Critical (>=95%), Percentage level of Max = 8000

Diagnostic Information:
The percent utilization of the Communication Agent User Data FIFO queue is approaching its defined capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new StackEvents (Query/Response/Relay) messages for the Task can be discarded, based on the StackEvent priority and Application's Global Congestion Threshold Enforcement Mode. This alarm should not normally occur when no other congestion alarms are asserted.

1. Recovery:

1. Navigate to **Alarms & Events** to examine the alarm log and determine if the ComAgent worker thread may be experiencing a problem preventing it from processing events from User Data FIFO queue.
2. Navigate to **Status & Manage**, and then **KPIs** to monitor the ingress traffic rate of each MP.
   - Mis-configuration of routing may result in unbalanced traffic directed to the MP. Under balanced traffic distribution, each MP should be receiving approximately the same ingress transaction per second.
   - There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
3. There may be an issue with network that causes lot of ComAgent connection setup and handshake messages. Check network latency and stability parameters.
4. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19808 - Communication Agent Connection FIFO Queue utilization

Alarm Group:
CAF

Description:
The percent utilization of the Communication Agent Connection FIFO queue is approaching defined threshold capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new ComAgent internal Connection Management StackEvents messages can be discarded based on Application's Global Congestion Threshold Enforcement Mode.

Severity:
Minor, Major, Critical

Instance:
<ComAgent StackTask Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFMxFIFOUtilNotify

Cause:
Minor (>= 60%), Major (>=80%), Critical (>=95%), Percentage level of Max = 1000

Diagnostic Information:
The percent utilization of the Communication Agent Connection FIFO queue is approaching its defined capacity. If this problem persists and the queue reaches above the defined threshold utilization, the new ComAgent internal Connection Management StackEvents messages can be discarded based on Application's Global Congestion Threshold Enforcement Mode. This alarm should not normally occur when no other congestion alarms are asserted.

1. Recovery:

1. Use **Main Menu**, and then **Alarms & Events** to determine if the ComAgent worker thread may be experiencing a problem preventing it from processing events from ComAgent Connection FIFO queue.

   It is recommended to contact My Oracle Supportfor assistance.

2. An IP network or adjacent node problem may exist preventing transmission of messages into the network at the same pace the messages are being received from the network.
3. Navigate to **Status & Manage**, and then **KPIs** to monitor the ingress traffic rate of each MP.
   - The mis-configuration of adjacent node IP routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
   - There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19810 - Communication Agent Egress Message Discarded

Event Type:
CAF

Description:
The **Communication Agent** egress message is being discarded due to one of the following reasons:

- Unknown destination server
- Connection state is not InService
- Incompatible destination
- Serialization failed
- MxEndpoint send failed
- Internal error

Severity:
Info

Instance:
<RemoteIP>

> **Note:**
>
> If <RemoteIP> is not known at the time of message discard, then "Unknown" will be used.

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventEgressMessageDiscardedNotify

1. Recovery:
1. View the Event AddlInfo column.

   Message is being discarded due to one of the reasons specified.
2. If it's a persistent condition with the status of one of the **Communication Agent** Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, It's an indication that the **Communication Agent** Process may be experiencing problems.
4. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log.
5. It is recommended to contact My Oracle Support for assistance.

19811 - Communication Agent Ingress Message Discarded

Event Type:
CAF

Description:
Communication Agent Ingress Message Discarded.

Severity:
Info

Instance:
<RemoteIP>

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventIngressMessageDiscardedNotify

1. Recovery:
1. View the Event AddlInfo column.

   Message is being discarded due to one of the reasons specified.
2. If it's a persistent condition with the status of one of the **Communication Agent** Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, it is an indication that the **Communication Agent** Process may be experiencing problems.
4. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log.
5. It is recommended to contact My Oracle Support for assistance.

19814 - Communication Agent Peer has not responded to heartbeat

Event Type:
CAF

Description:
Communication Agent Peer has not responded to heartbeat.

Severity:
Info

Instance:
<RemoteIP>

HA Score:
Normal

OID:
cAFEventHeartbeatMissedNotify

1. Recovery:
1. Check the configuration of managed objects and resolve any configuration issues with the Managed Object or hosting nodes.

   This message may be due to network condition or latency or due to setup issues.
2. If the event is raised due to software condition, It's an indication that the **Communication Agent** Process may be experiencing problems.
3. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log.
4. It is recommended to contact My Oracle Support for assistance.

19816 - Communication Agent Connection State Changed

Event Type:
CAF

Description:
Communication Agent Connection State Changed.

Severity:
Info

Instance:
<RemoteIP>

HA Score:
Normal

OID:
cAFEventConnectionStateChangeNotify

1. Recovery:

1. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log.

   This Event is a log of connection state change.

2. It is recommended to contact My Oracle Support for assistance.

19817 - Communication Agent DB Responder detected a change in configurable control option parameter

Event Type:
CAF

Description:
Communication Agent DB Responder detected a change in configurable control option parameter.

> **Note:**
>
> This event is an indication that **Communication Agent** detected a control parameter change. The change will be applied to applicable software component. If the change is applied on the GUI, the appropriate GUI action is logged in security logs. If the action is not performed from GUI and the control parameter is changed, this event indicates the executed change.

Severity:
Info

Instance:
N/A

HA Score:
Normal

OID:
cAFEventComAgtConfigParamChangeNotify

1. Recovery:

1. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log.

2. Use **Main Menu**, and then **Security Log** and examine the alarm log.

3. If the event shows up in **Main Menu**, and then **Alarms & Events**, without the corresponding GUI security-log in **Main Menu**, and then **Security Log**. It is recommended to contact My Oracle Support for assistance.

19818 - Communication Agent DataEvent Mempool utilization

Event Type:
CAF

Description:
The percent utilization of the Communication Agent DataEvent Mempool is approaching defined threshold capacity.

Severity:
Minor, Major, Critical

Instance:
<ComAgent Process>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFDataEvPoolResUtilNotify

1. Recovery:

- If the problem persists, it is recommended to contact My Oracle Support.

19820 - Communication Agent Routed Service Unavailable

Alarm Group:
CAF

Description:
This alarm indicates all connections of all connection groups associated with a routed service are unavailable. This generally occurs when far-end servers have been removed from service by maintenance actions. This can also occur if all of the routed service's connections have been either disabled or blocked.

Severity:
Major

Instance:
<RoutedServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFRSUnavailNotify

Cause:
When all member Connection Groups are Unavailable.

Diagnostic Information:
This alarm indicates all connections of all connection groups associated with a routed service are unavailable. This generally occurs when far-end servers have been removed from service by maintenance actions. This can also occur if all of the routed service's connections have been either disabled or blocked. Also, if there is any disruption that can lead to loss of connectivity between the user and provider MP.

1. Recovery:

1. Navigate to **Communication Agent**, and then **Maintenance**, and then **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** to view the reasons why connections are unavailable.
3. Navigate to **Status & Manage**, and then **Server** to confirm the far-end servers have an application state of enabled, and their subsystems are operating normally.

   This alarm can result from conditions at the far-end servers connected to the server that asserted this alarm.
4. Check network and reach-ability of provider server(s) from user server(s). Loss of network connectivity can lead to this alarm. In that case, the user also sees alarm 19800.
5. It is recommended to contact My Oracle Support for assistance.

19821 - Communication Agent Routed Service Degraded

Alarm Group:
CAF

Description:
This alarm indicates that some, but not all, connections are unavailable in the connection group being used by a Communication Agent Routed Service to route messages. The result is that the server that posted this alarm is not load-balancing traffic across all of the connections configured in the connection group.

Severity:
Major

Instance:
<ServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFRSDegradedNotify

1. Recovery:

1. Use **Communication Agent**, and then **Maintenance**, and then **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Communication Agent**, and then **Maintenance**, and then **Connection Status** to view the reasons why connections are unavailable.
3. Use **Status & Manage**, and then **Server** to confirm that the far-end servers have an application state of enabled, and that their subsystems are operating normally.

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.
4. It is recommended to contact My Oracle Support for assistance.

19822 - Communication Agent Routed Service Congested

Alarm Group:
CAF

Description:
This alarm indicates a routed service is load-balancing traffic across all connections in a connection group, but all of the connections are experiencing congestion. Messages may be discarded due to congestion.

Severity:
Major

Instance:
<ServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFRSCongestedNotify

Cause:
When the active Connection Group is congested.

Diagnostic Information:
This alarm indicates a routed service is load-balancing traffic across all connections in a connection group, but all of the connections are experiencing congestion. Messages may be discarded due to congestion. Congestion generally occurs when the far-end servers are overloaded.
Overload can be due to following:

- TCP connection has higher latency or error rate, then connection is getting into congestion state

- Far end server is receiving traffic at higher rate (may be from other servers). This triggers ComAgent congestion on far-end side.
- Application process CPU on far-end is above normal.

1. Recovery:

1. Navigate to **Communication Agent**, and then **Maintenance**, and then **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** to view the are congested and the degree to which they are congested.
3. Check the far-end of the congested connections to further isolate the cause of congestion.

   If the far-end servers are overloaded, then it is possible the system is being presented a load that exceeds its engineered capacity. If this is the case, then either the load must be reduced, or additional capacity must be added.
4. It is recommended to contact My Oracle Support for assistance.

19823 - Communication Agent Routed Service Using Low-Priority Connection Group

Alarm Group:
CAF

Description:
Communication Agent routed service is routing traffic using a connection group that has a lower-priority than another connection group.

Severity:
Major

Instance:
<ServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFRSUsingLowPriConnGrpNotify

1. Recovery:

1. Use **Communication Agent**, and then **Maintenance**, and then **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Communication Agent**, and then **Maintenance**, and then **Connection Status** to view the reasons why connections are unavailable.

3. Use **Status & Manage**, and then **Server** to confirm that the far-end servers have an application state of enabled, and that their subsystems are operating normally.

   It is possible that this alarm results from conditions at the far-end servers connected to the server that asserted this alarm.

4. It is recommended to contact My Oracle Support for assistance.

19824 - Communication Agent Pending Transaction Utilization

Alarm Group:
CAF

Description:
The **ComAgent** Reliable Transfer Function is approaching or exceeding its engineered reliable transaction handling capacity.

Severity:
Minor, Major, Critical

Instance:
N/A (ComAgent process)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFTransUtilNotify

Cause:
Default Values:

- Minor >= PTRCL1OnsetPrcnt and < PTRCL2OnsetPrcnt
- Major >= PTRCL2OnsetPrcnt and < PTRCL3OnsetPrcnt
- Critical >= PTRCL3OnsetPrcnt

Parameter Label	Description	Value Range	Default Value
PTRCL1AbatePrcnt (Minor)	Maximum quantity of allocated PTRs, in terms of a percentage of the maximum number supported, below which triggers the abatement of CL1 and onset of CL0. This value must be less than PTRCL1OnsetPrcnt.	1-99	50

PTRCL1OnsetPrcnt (Minor)	Minimum quantity of allocated PTRs, in terms of a percentage of the maximum number supported equal to or above which triggers the onset of PTR Resource Congestion Level 1 (CL1). This value must be less than or equal to PTRCL2OnsetPrcnt.	2-100	60
PTRCL2AbatePrcnt (Major)	Maximum quantity of allocated PTRs, in terms of a percentage of the maximum number supported, below which triggers the abatement of CL2 and onset of CL1. This value must be less than PTRCL2OnsetPrcnt.	1-99	70
PTRCL2OnsetPrcnt (Major)	Minimum quantity of allocated PTRs, in terms of a percentage of the maximum number supported equal to or above which triggers the onset of PTR Resource Congestion Level 2 (CL2). This value must be less than or equal to PTRCL2OnsetPrcnt.	2-100	90
PTRCL3AbatePrcnt (Critical)	Maximum quantity of allocated PTRs, in terms of a percentage of the maximum number supported, below which triggers the abatement of CL3 and onset of CL2. This value must be less than PTRCL3OnsetPrcnt.	1-99	90
PTRCL3OnsetPrcnt (Critical)	Minimum quantity of allocated PTRs, in terms of a percentage of the maximum number supported equal to or above which triggers the onset of PTR Resource Congestion Level 3 (CL3). This value must be less than or equal to PTRCL3OnsetPrcnt.	2-100	95

Diagnostic Information:
N/A.

1. Recovery:

1. Navigate to **Status & Manage**, and then **Server Status** to view **MP** server status.
2. Remote server is slow in responding to outstanding transaction with correlation resource in-use. The mis-configuration of **ComAgent** server/client routing may result in too much traffic being distributed to affected connection for MP.

3. There may be an insufficient number of server application MPs configured to handle the internal traffic load. If server application MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. Use **Alarm & Events** to examine the alarm log.

   The system may be experiencing network problems.

   The **Communication Agent** Process may be experiencing problems.
5. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19825 - Communication Agent Transaction Failure Rate

Alarm Group:
CAF

Description:
The number of failed transactions during the sampling period has exceeded configured thresholds.

Severity:
Minor, Major, Critical

Instance:
<ServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFTransFailRateNotify

Cause:
Default Values:

- Minor >= FailedTransOnset1Rate and < FailedTransOnset2Rate
- Major >= FailedTransOnset2Rate and < FailedTransOnset3Rate
- Critical >= FailedTransOnset3Rate

Parameter Label	Description	Value Range	Default Value
FailedTransAbate1Rate (Minor)	Threshold below which the Failed Transaction minor alarm is cleared.	1-99	4
FailedTransOnset1Rate (Minor)	Threshold equal-to or above which the Failed Transaction minor alarm is posted.	2-100	5
FailedTransAbate2Rate (Major)	Threshold below which the Failed Transaction major alarm is cleared.	1-99	6

FailedTransOnset2Rate (Major)	Threshold equal-to or above which the Failed Transaction major alarm is posted.	2-100	8
FailedTransAbate3Rate (Critical)	Threshold below which the Failed Transaction critical alarm is cleared.	1-99	9
FailedTransOnset3Rate (Critical)	Threshold equal-to or above which the Failed Transaction critical alarm is posted.	2-100	12

Diagnostic Information
N/A.

1. Recovery:

1. Navigate to **Status & Manage**, and then **Server Status** to view **MP** server status.
2. Remote server is slow in responding to outstanding transaction with correlation resource in-use. The mis-configuration of **ComAgent** Server/Client routing may result in too much traffic being distributed to affected connection for MP.
3. There may be an insufficient number of server application MPs configured to handle the internal traffic load. If server application MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. Navigate to **Alarm & Events** to examine the alarm log.

   The system may be experiencing network problems.

   The **Communication Agent** process may be experiencing problems.
5. It is recommended to contact My Oracle Support for assistance.

19826 - Communication Agent Connection Congested

Alarm Group:
CAF

Description:
This alarm indicates **Communication Agent** is experiencing congestion in communication between two servers and this can be caused by a server becoming overloaded or by network problems between two servers.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFConnCongestedNotify

Cause:

- A connection becomes congested, that is congestion level (CL) increases from ConnCL0 to either ConnCL1, ConnCL2, or ConnCL3. If a connection becomes congested, and there is another congested connection, then update the connection count and re-assert the alarm.
- A connection becomes uncongested, that is congestion level (CL) decreases to ConnCL0, and there is another congested connection. Update the connection count and re-assert the alarm.

Overload can be due to:

- TCP connection has higher latency or error rate, then connection is getting into congestion state
- Far-end server is receiving traffic at higher rate (may be from other servers). This triggers ComAgent congestion on far-end side.
- Application process CPU on far-end is above normal.

Diagnostic Information:
N/A.

1. Recovery:

1. Navigate to **Alarms & Events**, and then **View History** to find additional information for the alarm by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
2. Navigate to **Alarms & Events**, and then **View History** to check the event history logs for additional Communication Agent events or alarms from this MP server.
3. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine which connections on the server have abnormal status.
4. If the Remote MP Overload Level (OL) > 0 then determine why the remote server is congested.
    a. Verify the remote server is not under maintenance.
    b. Examine the remote's CPU utilization.
5. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19827 - SMS stack event queue utilization

Alarm Group:
SMS

Description:
The percent utilization of the SMS Task stack queue is approaching defined threshold capacity.

Severity:
Minor, Major, Critical

Instance:
<SMS Thread/Queue Index>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFSmsQueueUtilNotify

1. Recovery:

1. The system itself may be heavily loaded with work, causing this subsystem to also become overloaded. Check other system resources (ComAgent Congestion, Cpu Utilization, and Server Congestion are some examples) for signs of overload.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

19830 - Communication Agent Service Registration State Change

Event Type:
CAF

Description:
Communication Agent Service Registration State Change.

Severity:
Info

Instance:
<ServiceName>

HA Score:
Normal

OID:
cAFEventComAgtSvcRegChangedNotify

1. Recovery:

- This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.

19831 - Communication Agent Service Operational State Changed

Event Type:
CAF

Description:
Communication Agent Service Operational State Changed.

Severity:
Info

Instance:
<ServiceName>

HA Score:
Normal

OID:
cAFEventComAgtSvcOpStateChangedNotify

1. Recovery:

1. This event indicates that a **Communication Agent** service changed operational state, and typically results from maintenance actions.

   A service can also change state due to server overload.

2. If the state change is unexpected, it is recommended to contact My Oracle Support for assistance.

19832 - Communication Agent Reliable Transaction Failed

Event Type:
CAF

Description:
Failed transaction between servers result from normal maintenance actions, overload conditions, software failures, or equipment failures.

Severity:
Info

Instance:
<ServiceName>, <RemoteIP> |<null>

- If serviceID is InvalidServiceID, then <ServiceName> is “EventTransfer”.
- If <ServiceName> is “EventTransfer”, then include <RemoteIP>.
- If serviceID is unknown, then <ServiceName> is null.

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventComAgtTransFailedNotify

1. Recovery:

1. Use **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine if the local server is unable to communicate with another server or if servers have become overloaded.

2. Check the server’s KPIs and the **Communication Agent**, and then **Maintenance**, and then **Connection Status** to trouble-shoot the cause of server overload.

3. Check the **Communication Agent**, and then **Maintenance**, and then **HA Status** that corresponds to the ServiceID in the event instance to trouble-shoot the operation of the service.
4. If the event cannot be explained by maintenance actions, it is recommended to contact My Oracle Support for assistance.

19833 - Communication Agent Service Egress Message Discarded

Event Type:
CAF

Description:
Communication Agent Service Egress Message Discarded.

Severity:
Info

Instance:
<ServiceName>

- If serviceID is unknown, then <ServiceName> is null.

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventRoutingFailedNotify

1. Recovery:
1. View the Event AddlInfo column.

   Message is being discarded due to one of the reasons specified.
2. If it's a persistent condition with the status of one of the **Communication Agent** Configuration Managed Object then resolve the underlying issue with the Managed Object.
3. If the event is raised due to software condition, it's an indication that the **Communication Agent** Process may be experiencing problems.
4. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log.
5. It is recommended to contact My Oracle Support for assistance.

19842 - Communication Agent Resource-Provider Registered

Event Type:
CAF

Description:
Communication Agent Resource-Provider Registered.

Severity:
Info

Instance:
<ResourceName>

HA Score:
Normal

OID:
cAFEventResourceProviderRegisteredNotify

1. Recovery:

- No action required.

19843 - Communication Agent Resource-Provider Resource State Changed

Event Type:
CAF

Description:
Communication Agent Resource-Provider Resource State Changed.

Severity:
Info

Instance:
<ProviderServerName>: <ResourceName>

HA Score:
Normal

OID:
cAFEventResourceStateChangeNotify

1. Recovery:

- No action required.

19844 - Communication Agent Resource-Provider Stale Status Received

Event Type:
CAF

Description:
Communication Agent Resource-Provider Stale Status Received.

Severity:
Info

Instance:
<ProviderServerName>: <ResourceName>

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventStaleHBPacketNotify

1. Recovery:

- If this event is occurring frequently then check the **ComAgent** maintenance screens for other anomalies and to troubleshoot further.

19845 - Communication Agent Resource-Provider Deregistered

Event Type:
CAF

Description:
Communication Agent Resource-Provider Deregistered.

Severity:
Info

Instance:
<ResourceName>

HA Score:
Normal

OID:
cAFEventResourceProviderDeRegisteredNotify

1. Recovery:

- No action required.

19846 - Communication Agent Resource Degraded

Alarm Group:
CAF

Description:
Communication Agent Resource Degraded. A local application is using the resource, identified in the alarm, and the access to the resource is impaired. Some of the resource providers are either unavailable and/or congested.

Severity:
Major

Instance:
<ResourceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFResourceCongestedNotify

1. Recovery:

1. Use **Communication Agent**, and then **Maintenance**, and then **HA Services Status** to determine which sub-resources are unavailable or degraded for the server that asserted the alarm.
2. Use **Communication Agent**, and then **Maintenance**, and then **Connection Status** to determine if connections have failed or have congested.
3. It is recommended to contact My Oracle Support for assistance.

19847 - Communication Agent Resource Unavailable

Alarm Group:
CAF

Description:
Communication Agent Resource unavailable. A local application needs to use a **ComAgent** resource, but the resource is unavailable. The resource can be unavailable if the local server has no **ComAgent** connections to servers providing the resource or no servers host active instances of the resource's sub-resources.

Severity:
Major

Instance:
<ResourceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFResourceUnavailNotify

Cause:
Communication Agent Resource Unavailable. A local application needs to use a ComAgent resource, but the resource is unavailable. The resource can be unavailable if the local server has no ComAgent connections to servers providing the resource or no servers host active instances of the resource's sub-resources.

Diagnostic Information:
N/A.

1. Recovery:

1. Navigate to **Communication Agent**, and then **Maintenance**, and then **Connection Status** to verify the local server is connected to the expected servers.

   If the local server reports unavailable connections, then take actions to troubleshoot the cause of the connection failures.

2. If the **ComAgent** connections are InService, navigate to **Communication Agent**, and then **Maintenance**, and then **HA Services Status** to determine which servers are providing the resource.

   If no servers are providing the resource, then the most likely reason is maintenance actions have removed the application from service that provides the concerned resource.

3. It is recommended to contact My Oracle Support for assistance.

19848 - Communication Agent Resource Error

Alarm Group:
CAF

Description:
Communication Agent Resource Error. Two sets of servers are using incompatible configurations for a ComAgent resource.

Severity:
Minor

Instance:
<ResourceName>

HA Score:
Normal

Auto Clear Seconds:
50

OID:
cAFResourceErrorNotify

1. Recovery:

1. Use **Communication Agent**, and then **Maintenance**, and then **HA Services Status** to determine which sets of servers are incompatible.

   Check the incompatible servers to verify that they are operating normally and are running the expected versions of software.

2. It is recommended to contact My Oracle Support for assistance.

19850 - Communication Agent Resource-User Registered

Event Type:
CAF

Description:
Communication Agent Resource-User Registered.

Severity:
Info

Instance:
<ResourceName>

HA Score:
Normal

OID:
cAFEventResourceUserRegisteredNotify

1. Recovery:

- No action required.

19851 - Communication Agent Resource-User Deregistered

Event Type:
CAF

Description:
Communication Agent Resource-User Deregistered.

Severity:
Info

Instance:
<ResourceName>

HA Score:
Normal

OID:
cAFEventResourceUserDeRegisteredNotify

1. Recovery:

- No action required.

19852 - Communication Agent Resource Routing State Changed

Event Type:
CAF

Description:
Communication Agent Resource Routing State Changed.

Severity:
Info

Instance:
<ResourceName>

HA Score:
Normal

OID:
cAFEventResourceRoutingStateNotify

1. Recovery:

- No action required.

19853 - Communication Agent Resource Egress Message Discarded

Event Type:
CAF

Description:
Communication Agent Resource Egress Message Discarded.

Severity:
Info

Instance:
<ResourceName>: <SubResourceID>

> **Note:**
>
> If the resource is unknown, then <ResourceName> is the ResourceID converted to text. The <SubResourceID> is an integer converted to text, regardless of whether it is known or unknown.

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventHaEgressMessageDiscardedNotify

1. Recovery:
1. Message is being discarded due to one of the reasons specified in Event AddlInfo.

   If the condition is persistent with the status of one of the **ComAgent** Configuration Managed Objects there is an underlying issue with the Managed Object.
2. Use **Main Menu**, and then **Alarms & Events** and examine the alarm log for **ComAgent** Process problems.
3. It is recommended to contact My Oracle Support for assistance.

19854 - Communication Agent Resource-Provider Tracking Table Audit Results

Event Type:
CAF

Description:
Communication Agent Resource-Provider Tracking Table Audit Results. This event is generated when a **Resource Provider Tracking Table** (**RPTT**) entry with Status equal to Auditing is replaced with a new status (null, Active, Standby, Spare, OOS, etc) and there are no other RPTT entries, for this specific Resource/SR, with Status equal to Auditing.

Severity:
Info

Instance:
None

HA Score:
Normal

OID:
cAFEventHaRPTTAuditResultNotify

1. Recovery:

- No action required.

19855 - Communication Agent Resource Has Multiple Actives

Alarm Group:
CAF

Description:
This alarm indicates a possible IP network disruption that has caused more than one Resource Provider to become Active. The server that asserted this alarm expects there to be only one active Resource Provider server for the Resource, but instead it is seeing more than one. During this condition the server may be sending commands to the wrong Resource Provider. This may affect applications such as CPA, PDRA.

Severity:
Major

Instance:
<ResourceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFMultipleActivesNotify

1. Recovery:

1. Use **Communication Agent**, and then **Maintenance**, and then **HA Services Status** to determine which Resource Provider servers are announcing 'Active' status for the Resource.
2. Investigate possible IP network isolation between these Resource Provider servers.
3. It is recommended to contact My Oracle Support for assistance.

19856 - Communication Agent Service Provider Registration State Changed

Event Type:
CAF

Description:
The Communication Agent Service Provider Registration State has changed.

Severity:
Info

Instance:
<ServiceName>

HA Score:
Normal

OID:
cAFEventSvcProvRegStateChangedNotify

1. Recovery:

1. This event is a log of normal application startup and shutdown activity. It may provide aid during troubleshooting when compared to other events in the log.
2. It is recommended to contact My Oracle Support for further assistance.

19857 - Communication Agent Service Provider Operational State Changed

Event Type:
CAF

Description:
The Communication Agent Service Provider Operational State has Changed

Severity:
Info

Instance:
<ServiceName>

HA Score:
Normal

OID:
cAFEventSvcProvOpStateChangedNotify

1. Recovery:

1. This event indicates that a **ComAgent** service provider changed operational state, and typically results from maintenance actions. A service can also change state due to overload.
2. If the state change is unexpected, it is recommended to contact My Oracle Support.

19858 - Communication Agent Connection Rejected

Event Type:
CAF

Description:
The Communication Agent receives a connection request from an unknown server.

Severity:
Info

Instance:
<RemoteIP>

HA Score:
Normal

Throttle Seconds:
1800 (30 minutes)

OID:
cAFEventSvcProvOpStateChangedNotify

1. Recovery:

1. Verify network routes are correctly configured for ComAgent.
2. If assistance is required, it is recommended to contact My Oracle Support.

19860 - Communication Agent Configuration Daemon Table Monitoring Failure

Alarm Group:
CAF

Description:
This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology

configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
CAFTableMonitorFailureNotify

Cause:
Alarm 19860 is asserted when Communication Agent Configuration Daemon is unable to monitor one or more tables that it has been configured to monitor.

Diagnostic Information:
This alarm indicates that a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

To troubleshoot:

- Find additional information for the alarm in **Alarms & Events**, and then **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
- Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this server.

1. Recovery:

1. Use **Alarms & Events**, and then **View History** to find additional information about the alarm.

   The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.

2. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this MP server.
3. If conditions do not permit a forced failover of the active NOAM, it is recommended to contact My Oracle Support for assistance.
4. If conditions permit, then initiate a failover of active NOAM.

   This causes the Communication Agent Configuration Daemon to exit on the originally-active NOAM and to start on the newly-active NOAM.
5. After NOAM failover completes, verify the alarm has cleared.
6. If the alarm has not cleared, it is recommended to contact My Oracle Support for assistance.

19861 - Communication Agent Configuration Daemon Script Failure

Alarm Group:
CAF

Description:
This alarm indicates a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFScriptFailureNotify

Cause:
This alarm raises when the Communication Agent Configuration Daemon configuration script fails.

Diagnostic Information:
This alarm indicates a Communication Agent Configuration Daemon has encountered an error that prevents it from properly using server topology configuration data to configure automatic connections for the Communication Agents on MPs, and this may prevent applications on MPs from communicating.

To troubleshoot:

- Find additional information for the alarm in **Alarms & Events**, and then **View History** by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.
- Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this server.

1. Recovery:

1. Use **Alarms & Events**, and then **View History** to find additional information about the alarm.

   The information can be found by locating the row with a sequence number that matches the active alarm sequence number and viewing the Additional Info column.

2. Check the event history logs at **Alarms & Events**, and then **View History** for additional Communication Agent events or alarms from this server.

3. If conditions do not permit a forced failover of the active NOAM, it is recommended to contact My Oracle Support for assistance.
4. If conditions permit, then initiate a failover of active NOAM.

   This causes the Communication Agent Configuration Daemon to exit on the originally-active NOAM and to start on the newly-active NOAM.
5. After NOAM failover completes, verify the alarm has cleared.
6. If the alarm has not cleared, it is recommended to contact My Oracle Support for assistance.

19862 - Communication Agent Ingress Stack Event Rate

Alarm Group:
CAF

Description:
The Communication Agent Ingress Stack Event Rate is approaching its defined threshold capacity.

Severity:

- Minor - if exceeding 100K on Gen8/Gen9 hardware, 75k on other hardware
- Major - if exceeding 110K on Gen8/Gen9 hardware, 80k on other hardware
- Critical - if exceeding 120K on Gen8/Gen9 hardware, 84k on other hardware

Instance:
<ServiceName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
cAFIngressRateNotify

1. Recovery:
1. This alarm indicates that a server is overrunning its defined processing capacity. If any of the defined threshold onset levels are exceeded, Communication Agent will discard comparatively low priority messages. Check the configuration, routing, and deployment mode capacity.
2. It is recommended to contact My Oracle Support for further assistance.

19863 - Communication Agent Max Connections Limit In Connection Group Reached

Event Group:
CAF

Description:
The maximum number of connections per connection group limit has been reached.

Severity:
Info

Instance:
<Connection group name>

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFComAgentMaxConnsInConnGrpNotify

1. Recovery:

1. This event indicates that a connection group has already reached its maximum limit and no more connections can be added to the group. Determine what is preventing potential connections from being added to the connection group.
2. It is recommended to contact My Oracle Support for further assistance.

19864 - ComAgent Successfully Set Host Server Hardware Profile

Event Group:
CAF

Description:
ComAgent successfully set the host server hardware profile.

Severity:
Info

Instance:
None

HA Score:
Normal

OID:
cAFEventSuccessSetHostServerHWProfileNotify

1. Recovery:

1. This event indicates that all TPS controlling parameter values are successfully set for the host server hardware profile.
2. If needed, it is recommended to contact My Oracle Support.

19865 - ComAgent Failed to Set Host Server Hardware Profile

Event Group:
CAF

Description:
ComAgent failed to set the host server hardware profile.

Severity:
Info

Instance:
None

HA Score:
Normal

OID:
cAFEventFailToSetHostServerHWProfileNotify

1. Recovery:

1. This event indicates that there is a failure in applying default hardware settings for ComAgent TPS controlling parameters. When default settings also fail to apply, then the factory values will be used for the TPS controlling parameters.
2. If needed, it is recommended to contact My Oracle Support.

19866 - Communication Agent Peer Group Status Changed

Event Type:
CAF

Description:
The Communication Agent Peer Group operational status has changed.

Severity:
Info

Instance:
<PeerGroupName>

HA Score:
Normal

OID:
cAFEventPeerGroupStatusChangeNotify

1. Recovery:

- This alarm is informational and no action is required.

19867 - Communication Agent Peer Group Egress Message Discarded

Event Type:
CAF

Description:
The Communication Agent Peer Group egress message is being discarded due to one of the following reasons:

- Unknown Peer Group
- Peer Group Unavailable
- Peer Congested
- Reliability not supported

Severity:
Info

Instance:
<PeerGroupName>

HA Score:
Normal

Throttle Seconds:
10

OID:
cAFEventPSEgressMessageDiscardedNotify

1. Recovery:

- This alarm is informational and no action is required.

19868 - Communication Agent Connection Rejected - Incompatible Network

Event Type:
CAF

Description:
Communication Agent connection rejected. Connection to the peer node is not initiated due to network incompatibility. This event will be raised on the connection initiator side when the connection initiator MP has only IPv6 IP addresses configured and Remote MP has only IPv4 IP addresses configured or when connection initiator MP has only IPv4 IP addresses configured and Remote MP has only IPv6 IP addresses configured.

Severity:
Info

Instance:
<RemoteIP>

HA Score:
Normal

OID:
cAFEventConnectionRejectNotify

1. Recovery:

1. Disable both sides of the connection.
2. Configure the correct network modes on either server.
3. Restart the application on the reconfigured server.
4. Enable both sides of the connection.
5. It is recommended to contact My Oracle Support for assistance if needed.

19900 - Process CPU Utilization

Alarm Group:
STK

Description:
The process, which is responsible for handling all signaling traffic, is approaching or exceeding its engineered traffic handling capacity.

Severity:
Critical, Major, Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
dbcProcessCpuUtilizationNotify

Cause:
This alarm raises when the MP is handling too much traffic and is operating in congestion.

Diagnostic Information:
N/A

1. Recovery:

1. Navigate to **Status & Manage**, and then **KPIs** to monitor the ingress traffic rate of each MP.
   - The mis-configuration of Server/Client routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
   - There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state, then the traffic load to the server site is exceeding its capacity.
2. Navigate to **Alarms & Events** to examine the alarm log.

   It is recommended to contact My Oracle Support for assistance.

19901 - CFG-DB Validation Error

Alarm Group:
STK

Description:
A minor database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
dbcCfgDbValidationErrorNotify

1. Recovery:

- An unexpected condition has occurred while performing a database update, but database updates are still enabled.

  It is recommended to contact My Oracle Support for assistance.

19902 - CFG-DB Update Failure

Alarm Group:
STK

Description:
A critical database validation error was detected on the MP server during an update. MP internal database is now out of sync with the configuration database. Subsequent database operations on the MP are DISABLED.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
dbcCfgDbUpdateFailureNotify

Cause:
After receiving configuration updates from GUI, the DSR application is not able to modify its Runtime Database completely and correctly. All configurations changes are verified for syntactic and semantic errors by pre-update procedures.
Poor system health or degraded application state might be one of the cause.

Diagnostic Information:

- Determine if this condition indicates a software problem or unexpected TC User behavior.
- The Event Additional Information field includes a description of the event received, cause, and the actions occurred with the operation or dialogue as a result. Dialogue removed by dialogue cleanup timer.
- Possibly an Internal Error has occurred. Perform the following:
  - Click Alarm Instance.
  - Collect the information from instance and additional Information section of raised alarm.
  - Provide this information while contacting My Oracle Support.

1. Recovery:

- An unexpected condition has occurred while performing a database update and database updates are disabled. Try to revert back a configuration change if possible.

  It is recommended to contact My Oracle Support for assistance.

19903 - CFG-DB post-update Error

Alarm Group:
STK

Description:
A minor database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are ALLOWED.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
dbcCfgDbPostUpdateErrorNotify

Cause:
N/A

Diagnostic Information:
N/A

1. Recovery:

- An unexpected condition has occurred while performing a database update, but database updates are still enabled.

  It is recommended to contact My Oracle Support for assistance.

19904 - CFG-DB Post-Update Failure

Alarm Group:
STK

Description:
A critical database validation error was detected on the MP server after a database update. MP internal database is still in sync with the configuration database. Subsequent database operations on the MP are DISABLED.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
dbcCfgDbPostFailureNotify

Cause:
After receiving configuration updates from GUI, the DSR application is not able to modify its Runtime Database and fails in the post-update procedure such as verification. The error is critical, and subsequent configuration updates will not be updated in the Runtime Database.
All configurations changes are verified for syntactic and semantic errors by pre-update procedures. One of the causes for this alarm is the poor system health.

Diagnostic Information:
The alarm may raise due to an internal error. Click **Alarm Instance**. Collect the information from instance and additional Information section of raised alarm. Provide this information while contacting My Oracle Support.

1. Recovery:

- An unexpected condition has occurred while performing a database update and database updates are disabled. Try to revert back a configuration change if possible.

It is recommended to contact My Oracle Support for assistance.

19905 - Measurement Initialization Failure

Alarm Group:
STK

Description:
A measurement object failed to initialize.

Severity:
Critical

Instance:
<measTagName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
dbcMeasurementInitializationFailureNotify

Cause:
All Measurements are bound to a specific Measurement ID or Measurement Name defined in the Internal Database. This alarm is raised when Measurement subsystem initialization has failed, which occurs only when the system (or a process) is coming up.
The alarm raises when:

- An application is trying to bind the measurement using an incorrect measurement identifier which does not exist in Database. If you have performed an upgrade or a new installation, contact My Oracle Support for assistance.
- An unauthorized configuration change resulted in inconsistent data.

Diagnostic Information:
Note any configuration change made to the system which requires (or caused) a process(or system) restart. Additionally, note alarm instance and any additional information present in alarm's **Additional Info** section.

1. Recovery:

- Measurement subsystem initialization has failed for the specified measurement. If alarm is raised after a configuration change, try to revert back the configuration and restart the process that raised the alarm.

  If configuration changes were valid and authorized, it is recommended to contact My Oracle Support for assistance.

Diameter Signaling Router (DSR) Diagnostics (19910-19999)

This section provides information and recovery procedures for **DSR** alarms and events, ranging from 19910-19999, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the Alarms & Events > View History page.

19910 - Message Discarded at Test Connection

Event Type:
DIAG

Description:
Normal traffic is being discarded because it is routed to an egress Test Connection. An egress Test Connection is given a normal message to be transmitted.

Severity:
Major

Instance:
<Connection name>

HA Score:
Normal

Auto Clear Seconds:
120

OID:
dbcNormalMessageDiscardedNotify

1. Recovery:
1. Update routing rules to exclude Test connections from being used for routing.

   Normal traffic should be received and sent on non-test connections.
2. Change the hostname of the peer connected to the test connection.

   The hostname of the peer connected to the test connection may be the destination host for the incoming normal traffic.

19911 - Test message discarded

Event Type:
DIAG

Description:
Test message is given to a non-test connection to be transmitted.

Severity:
Info

Instance:
<Connection name>

HA Score:
Normal

Throttle Seconds:
5

OID:
dbcDiagnosticMessageDiscardNotify

1. Recovery:

- Update routing rules to exclude Test messages from being routed to non-test connection.

  Test messages should be received and sent only on test connections.

Diameter Alarms and Events (8000-8299, 22000-22350, 22900-22999, 25600-25899)

8000 - MpEvFsmException

8000 - 001 - MpEvFsmException_SocketFailure

Event Type:
DIAM

Description:
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

1. This event is potentially caused by the Peer CNDRA process reaching its descriptor capacity.

2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 002 - MpEvFsmException_BindFailure

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery
1. Potential causes of this event are:
   - Network interface(s) are down.
   - Port is already in use by another process.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 003 - MpEvFsmException_OptionFailure

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:003

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

1. Potential causes of this event are:
   - Peer CNDRA process is not running with root permission.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 004 - MpEvFsmException_AcceptorCongested

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:004

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- This event is potentially caused by a network or upgrade event that resulted in a synchronization of peer connection attempts.

> **Note:**
>
> The rate will ease over time as an increasing number of connections are accepted.

8000 - 101 - MpEvFsmException_ListenFailure

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 102 - MpEvFsmException_PeerDisconnected

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- No action required.

8000 - 103 - MpEvFsmException_PeerUnreachable

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:103

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- Potential causes for this event are:
  - A host IP interface is down.
  - A host IP interface is unreachable from the peer.
  - A peer IP interface is down.
  - A peer IP interface is unreachable from the host.

8000 - 104 - MpEvFsmException_CexFailure

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:104

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- Potential causes for this event are:
  - The peer is misconfigured.
  - The host is misconfigured.

8000 - 105 - MpEvFsmException_CerTimeout

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:105

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- No action required.

8000 - 106 - MpEvFsmException_AuthenticationFailure

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:106

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery

- Potential causes for this event are:
  - The peer is misconfigured.

- The host is misconfigured.

8000 - 201 - MpEvFsmException_UdpSocketLimit

Event Type
DIAM

Description
DraWorker connection FSM exception.

Severity
Info

Instance
<DraWorker Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

1. Recovery:

- The Peer CNDRA supports to a preconfigured maximum number of open UDP sockets. One or more peers are being routed more traffic than is normally expected, or the peers are responding slowly, causing more than the usual number of UDP sockets being opened. The concerned peer can be identified using the reported connection ID. Investigate the reason for higher than normal traffic being forwarded to the peer, or why the peer is slow to respond.

8001 - MpEvException

8001 - 001 - MpEvException_Oversubscribed

Event Type
DIAM

Description
DraWorker exception.

Severity
Info

Instance
<DraWorker Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterMpEvException

1. Recovery

- Bounce one or more floating connections to force their migration to another DraWorker with available capacity.

8002 - MpEvRxException

8002 - 001 - MpEvRxException_DiamMsgPoolCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- Potential causes of this event are:
  - One or more DraWorkers are unavailable and traffic has been distributed to the remaining DraWorkers.
  - One or more peers are generating more traffic than is nominally expected.
  - There are an insufficient number of DraWorkers provisioned.
  - One or more peers are answering slowly, causing a backlog of pending transactions.

8002 - 002 - MpEvRxException_MaxMpsExceeded

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is potentially caused when a peer is generating more traffic than is nominally expected.

8002 - 003 - MpEvRxException_CpuCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:003

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- Potential causes for this event are:
  - One or more peers are generating more traffic than is nominally expected.
  - Configuration requires more CPU for message processing than is nominally expected.
  - One or more peers are answering slowly, causing a backlog of pending transactions

8002 - 004 - MpEvRxException_SigEvPoolCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:004

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 005 - MpEvRxException_DstMpUnknown

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:005

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 006 - MpEvRxException_DstMpCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:006

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- Potential causes for this event are:
  - One or more peers are generating more traffic than is nominally expected.
  - Configuration requires more CPU for message processing than is nominally expected.
  - One or more peers are answering slowly, causing a backlog of pending transactions.

8002 - 007 - MpEvRxException_DrlReqQueueCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:007

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 008 - MpEvRxException_DrlAnsQueueCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:008

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 009 - MpEvRxException_ComAgentCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:009

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 201 - MpEvRxException_MsgMalformed

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8002 - 202 - MpEvRxException_PeerUnknown

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery

- The host or peer may be misconfigured. Adjust the peer IP address(es) option of the associated Peer Node if necessary.

8002 - 203 - MpEvRxException_RadiusMsgPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. **MP** server status can be monitored from the **Status & Manage**, and then **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each **MP** can be monitored from the **Status & Manage**, and then **KPIs** page. Each **MP** in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each **MP** can be monitored from the **Status & Manage**, and then **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined using the Alarms & Events page.
5. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 204 - MpEvRxException_ItrPoolCongested

Event Type
DIAM

Description
DraWorker ingress message processing exception.

Severity
Info

Instance
<DraWorker Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery:

1. Adjust the RADIUS **Cached Response Duration** option of the associated Connection configuration set(s) to reduce the lifetime of cached transactions, if needed.
2. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
3. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
4. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
5. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined.
6. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 205 - MpEvRxException_RclRxTaskQueueCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery:

1. The alarm will clear when the DCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 206 - MpEvRxException_RclSigEvPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:206

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage**, and then **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined using the **Alarms & Events** page.
5. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 207 - MpEvRxException_ReqDuplicate

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:207

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery:
1. It is possible to observe this event occasionally, due to the unreliable nature of the UDP transport protocol. However, if the occurrence of this event is frequent, investigate the issue further.

   This event is expected when a retransmission is received from the client before a server has responded to the request, possibly a result of the client retransmitting too quickly before allowing sufficient time for a server to respond in time. Another possible cause is if one or more servers configured to handle the request are non-responsive.
2. Investigate the routing configuration to narrow down the list of servers (Peer Nodes) which are expected to handle requests from the reported server connection.
3. Evaluate whether an Egress Transaction Failure Rate alarm has been raised for any of the corresponding client connections. If so, investigate the cause of the server becoming non-responsive and address the condition.

> **Note:**
>
> Depending on the operator's choice, the client connection may need to be Admin Disabled until the evaluation is complete, which will allow requests to be routed to other servers, depending on the routing configuration. If this is not the case, tune the client's retransmit timers to be greater than the typical turnaround time for the request to be processed by the server and for the response to be sent back to the client.

4. If the problem persists, it is recommended to contact My Oracle Support.

8002 - 208 - MpEvRxException_SharedSecretUnavailable

Event Type
DIAM

Description
Failed to access shared secret.

Severity
Info

Instance
<Connection Name>:208

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

1. Recovery:

- Check to see if alarm 8207 is present. If so, follow the recovery steps for alarm 8207 - MpRadiusKeyError.

8003 - MpEvTxException

8003 - 001 - MpEvTxException_ConnUnknown

Event Type
DIAM

Description
DraWorker egress message processing exception.

Severity
Info

Instance
<DraWorker Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery

- No action required.

8003 - 101 - MpEvTxException_DclTxTaskQueueCongested

Event Type
DIAM

Description
DraWorker egress message processing exception.

Severity
Info

Instance
<DraWorker Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery

- This event is potentially caused by one or more peers being routed more traffic than is nominally expected.

8003 - 201 - MpEvTxException_RclTxTaskQueueCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery:

1. The alarm will clear when the DCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8003 - 202 - MpEvTxException_EtrPoolCongested

Event Type
DIAM

Description
DraWorker egress message processing exception.

Severity
Info

Instance
<DraWorker Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery:

1. Adjust the Diameter configuration set(s) to reduce the lifetime of pending transactions, if needed.
2. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
3. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
4. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

5. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted.
6. If the problem persists, it is recommended to contact My Oracle Support.

8003 - 203 - MpEvTxException_RadiusMsgPoolCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage**, and then **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined using the **Alarms & Events** page.
5. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8003 - 204 - MpEvTxException_RadiusIdPoolCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery:

1. The peer is being routed more traffic than is nominally expected, or is responding slowly. If the problem persists, the client port range configured in the Local Node corresponding to the indicated transport connection may need to be increased.
2. Access the connection information via **Diameter**, and then **Configuration**, and then **Connections** screen, which indicates the associated Local Node.
3. Access the Local Node screen via **Diameter**, and then **Configuration**, and then **Local Nodes**.
4. Update the client port range by modifying the **RADIUS Client UDP Port Range Start** and the **RADIUS Client UDP Port Range End** values in the Local Node edit screen, if necessary.

> **Note:**
>
> To update the Local Node configuration, Admin Disable all associated connections.

8003 - 205 - MpEvTxException_SharedSecretUnavailable

Event Type
DIAM

Description
Failed to access shared secret.

Severity
Info

Instance
<DA-MP Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

1. Recovery:

1. Proceed to 2 if alarm 8207 - MpRadiusKeyError is present.
2. Synchronize the RADIUS key file.
3. Restart the DSR process. If the required keys are now available, the alarm will not be raised.
4. If the problem persists, it is recommended to contact My Oracle Support.

8004 - EvFsmAdState

8004 - 001 - EvFsmAdState_StateChange

Event Type
DIAM

Description
Connection FSM administrative state change.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterEvFsmAdState

1. Recovery

- No action required.

8005 - EvFsmOpState

8005 - 001 - EvFsmOpState_StateChange

Event Type
DIAM

Description
Connection FSM operational state change.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterFsmOpState

1. Recovery

1. No action required when operationally available.
2. Potential causes for this event when operationally unavailable are:
   - Connection is administratively disabled.
   - Diameter initiator connection is connecting.
   - Diameter initiator connection is suppressed (peer is operationally available).
   - Diameter initiator connection is suppressed (peer did not signal reboot during graceful disconnect).
   - Diameter responder connection is listening.
   - RADIUS server connection is opening.
3. Potential causes for this event when operationally degraded are:
   - Connection egress message rate threshold crossed.
   - Diameter connection is in watchdog proving.
   - Diameter connection is in graceful disconnect.
   - Diameter peer signaled remote busy.
   - Diameter connection is in transport congestion.

8006 - EvFsmException

8006 - 001 - EvFsmException_DnsFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- Potential causes of this event are:
  - DNS server configuration is invalid.
  - DNS server(s) are unavailable.
  - DNS server(s) are unreachable.
  - FQDN configuration is invalid.

8006 - 002 - EvFsmException_ConnReleased

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- No action required.

8006 - 101 - EvFsmException_SocketFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

1. This event is potentially caused by the Peer CNDRA process reaching its descriptor capacity.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 102 - EvFsmException_BindFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

1. Potential causes for this event are:
   - Network interface(s) are down.
   - Port is already in use by another process.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 103 - EvFsmException_OptionFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:103

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery
1. Potential causes for this event are:
   - Peer CNDRA process is not running with root permission.
   - Configuration is invalid.
2. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 104 - EvFsmException_ConnectFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:104

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8006 - 105 - EvFsmException_PeerDisconnected

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:105

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- No action required. Potential causes for this event are:
  - Diameter peer signaled **DPR**.
  - Peer is unavailable.

8006 - 106 - EvFsmException_PeerUnreachable

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:106

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- Potential causes for this event are:
  - A host IP interface is down.
  - A host IP interface is unreachable from the peer.
  - A peer IP interface is down.
  - A peer IP interface is unreachable from the host.

8006 - 107 - EvFsmException_CexFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:107

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- Potential causes for this event are:
  - The peer is misconfigured.
  - The host is misconfigured.

8006 - 108 - EvFsmException_CeaTimeout

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:108

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- No action required.

8006 - 109 - EvFsmException_DwaTimeout

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:109

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- No action required.

8006 - 110 - EvFsmException_DwaTimeout

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:110

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- No action required.

8006 - 111 - EvFsmException_ProvingFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:111

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- Potential causes for this event are:
  - A host IP interface is unreachable from the peer, or intermittently so.
  - A peer IP interface is unreachable from the host, or intermittently so.

8006 - 112 - EvFsmException_WatchdogFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:112

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- Potential causes for this event are:
  - A host IP interface is unreachable from the peer, or intermittently so.
  - A peer IP interface is unreachable from the host, or intermittently so.

8006 - 113 - EvFsmException_AuthenticationFailure

Event Type
DIAM

Description
Connection FSM exception.

Severity
Info

Instance
<Connection Name>:113

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvFsmException

1. Recovery

- Potential causes for this event are:
  - The peer is misconfigured.
  - The host is misconfigured.

8007 - EvException

8007 - 101 - EvException_MsgPriorityFailure

Event Type
DIAM

Description
Connection exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvException

1. Recovery

- This event is potentially caused by misconfiguration of the host.

8008 - EvRxException

8008 - 001 - EvRxException_MaxMpsExceeded

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery

- This event is potentially caused when a peer is generating more traffic than is nominally expected.

8008 - 101 - EvRxException_MsgMalformed

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8008 - 102 - EvRxException_MsgInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8008 - 201 - EvRxException_SharedSecretUnavailable

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 202 - EvRxException_MsgAttrLenUnsupported

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 203 - EvRxException_MsgTypeUnsupported

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect or may be misconfigured.

8008 - 204 - EvRxException_AnsOrphaned

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- The peer is responding slowly, network latency is high, or the ETR timer is configured too small. Adjust the Diameter configuration set(s) to reduce the lifetime of pending transactions, if needed.

8008 - 205 - EvRxException_AccessAuthMissing

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 206 - EvRxException_StatusAuthMissing

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:206

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8008 - 207 - EvRxException_MsgAuthInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:207

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

1. Evaluate the indicated message. If an invalid message authenticator value is indicated, ensure that the same shared secret is configured for the connection on the Peer CNDRA and on the RADIUS peer.
2. If an invalid message authenticator value is not indicated, then the peer may have an implementation defect or may be misconfigured. It is recommended to contact My Oracle Support for assistance. This event is unexpected.

8008 - 208 - EvRxException_ReqAuthInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:208

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.

8008 - 209 - EvRxException_AnsAuthInvalid

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:209

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.

8008 - 210 - EvRxException_MsgAttrAstUnsupported

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:210

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect or may be misconfigured .
2. Only certain Acct-Status-Type values are supported. Ensure that the Acct-Status-Type value is one of these values:
   - 1 (Start)
   - 2 (Stop)
   - 3 (Interim-Update)
   - 7 (Accounting-On)
   - 8 (Accounting-Off)

8008 - 212 - EvRxException_MsgTypeMissingMccs

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:212

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- It is recommended to contact My Oracle Support for assistance. The peer or host is misconfigured.

8008 - 213 - EvRxException_ConnUnavailable

Event Type
DIAM

Description
Connection ingress message processing exception.

Severity
Info

Instance
<Connection Name>:213

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvRxException

1. Recovery:

- No action required. This event is for informational purposes only.

8009 - EvTxException

8009 - 001 - EvTxException_ConnUnavailable

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery

- No action required.

8009 - 101 - EvTxException_DclTxConnQueueCongested

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery

- This event is potentially caused by a peer being routed more traffic than is nominally expected.

8009 - 102 - EvTxException_DtlsMsgOversized

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery

- This event is potentially caused by a peer being routed more traffic than is nominally expected.

8009 - 201 - EvTxException_MsgAttrLenUnsupported

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect.

8009 - 202 - EvTxException_MsgTypeUnsupported

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

- This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may have an implementation defect, or may be misconfigured.

8009 - 203 - EvTxException_MsgLenInvalid

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:203

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.
2. This event is typically generated when the Peer CNDRA needs to add a Message-Authenticator to the message, but doing so causes the message size to exceed maximum RADIUS message length. If this problem persists, evaluate the source of this message and ensure that the message size allows adding a Message-Authenticator attribute (16 octets). Evaluate the message authenticator configuration for the egress connection and ensure that the adding of Message-Authenticator to specific message types is configured appropriately.

8009 - 204 - EvTxException_ReqOnServerConn

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Review the configuration of Route Groups and ensure that there are no RADIUS server instances.

8009 - 205 - EvTxException_AnsOnClientConn

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:205

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Review the configuration of Connections and ensure that there are no RADIUS client instances being used as a RADIUS server by one or more peers.

8009 - 206 - EvTxException_DiamMsgMisrouted

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:206

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Review the configuration of Route Groups and ensure that there are no RADIUS server instances.

8009 - 207 - EvTxException_ReqDuplicate

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:207

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

- No action required.

8009 - 208 - EvTxException_WriteFailure

Event Type
DIAM

Description
Connection egress message processing exception.

Severity
Info

Instance
<Connection Name>:208

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterEvTxException

1. Recovery:

1. This event is unexpected. It is recommend to contact My Oracle Support for assistance. The peer may be misconfigured.
2. Ensure that the RADIUS **UDP Transmit Buffer Size** is sufficient for the offered traffic load.

8010 - MpIngressDrop

Alarm Group:
DIAM

Description:
An ingress message is discarded or rejected.

Severity:
Major

Instance:
<DraWorker Name>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
eagleXgDiameterMpIngressDrop

Cause:
An ingress message is discarded or rejected in the following congestion scenarios:

- Connection maximum message rate exceeded (ingress control).
- DraWorker maximum message rate exceeded (ingress control).
- DraWorker CPU congestion (overload control).
- Diameter message pool congested (routing ingress).
- Signaling event pool congested (routing ingress).
- Destination DraWorker unknown (routing ingress).
- Destination DraWorker congested (routing ingress).

- DRL request message queue congested (routing ingress).
- DRL answer message queue congested (routing ingress).

Diagnostic Information:
Collect the following information to diagnose the cause before contacting Oracle Support:

- Event History on active SO server.
- Savelogs of all MPs.
- Peer CNDRA logs of all MPs.

1. Recovery:

- Potential causes of this alarm are:
  - One or more DraWorkers are unavailable and traffic has been distributed to the remaining DraWorkers.
  - One or more peers are generating more traffic than is nominally expected.
  - There are an insufficient number of DraWorkers provisioned.
  - One or more peers are answering slowly, causing a backlog of pending transactions.

8011 - EcRate

Alarm Group:
DIAM

Description:
Connection egress message rate threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEmr

Cause:
Connection egress message rate threshold crossed.

Diagnostic Information:
Collect the following information to diagnose the cause before contacting Oracle Support:

- Event History on active SO server.

- Savelogs of the MP server.
- Peer CNDRA logs of the MP server.

1. Recovery:

1. This alarm is potentially caused when a peer has routed more traffic than is nominally expected.
2. Inability of the adjacent Diameter Peer to handle the rate of egress message traffic currently being offered on a connection.
3. TCP/SCTP buffers filling up on the egress side.

8012 - MpRxNgnPsOfferedRate

Alarm Group:
DIAM

Description:
DraWorker ingress NGN-PS message rate threshold crossed.

Severity:
Major

Instance:
MpRxNgnPsOfferedRate, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpRxNgnPsOfferedRateNotify

Cause:
DraWorker ingress NGN-PS message rate threshold crossed. The alarm clears when threshold crossing abates.

Diagnostic Information:
N/A

1. Recovery:

1. Check for one or more DraWorkers is unavailable and traffic has been distributed to the remaining DraWorkers.
2. Check for one or more peers is generating more traffic than is nominally expected.
3. Check for an insufficient number of DraWorkers provisioned.
4. This alarm clears when the treshold crossing abates.

8013 - MpNgnPsStateMismatch

Alarm Group:
DIAM

Description:
DraWorker NGN-PS administrative and operational state mismatch.

Severity:
Major

Instance:
<DraWorker Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpNgnPsStateMismatch

Cause:
The alarm raises when the administrative state of NGN-PS is not aligned with the operational state. Alarm clears when the administrative and operational states are aligned.

Diagnostic Information:
Collect the following information to diagnose the cause before contacting Oracle Support:

- The details of active SO server.
- Event History on active SO server.

1. Recovery:

1. This alarm is potentially caused when a DraWorker restart is required.

   The alarm clears when the administrative and operational states are aligned.

2. If the NGN-PS feature is mistakenly activated, disable the feature to clear the alarm and align the operational state with administrative state .
3. If the NGN-PS feature is mistakenly de-activated, enable the feature to clear the alarm and align the operational state with administrative state.

8014 - MpNgnPsDrop

Alarm Group:
DIAM

Description:
DraWorker NGN-PS message discarded or rejected.

Severity:
Major

Instance:
<DraWorker Name>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
eagleXgDiameterMpNgnPsDrop

Cause:
Each layer involved in processing an NGN-PS transaction may reject or discard a request or answer. Such scenarios include:

- Routing or application controls.
- Peer or network congestion.
- Internal processing error.
- Task queue or resource congestion or ComAgent congestion or delivery failure.
- Processing error.

Diagnostic Information:
Collect the following information to diagnose the cause before contacting Oracle Support:

- Event History on active SO server.
- Savelogs of all MPs.
- DSR logs of all MPs.

1. Recovery

- Potential causes of this alarm are:
  - Routing or application controls are configured incorrectly.
  - Peer or network is in congestion.
  - Engineering of internal resources is insufficient.

8015 - NgnPsMsgMisrouted

Alarm Group:
DIAM

Description:
NGN-PS message routed to peer CNDRA lacking NGN-PS support.

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds
30

OID:
eagleXgDiameterNgnPsMsgMisrouted

Cause:
An NGN-PS message routed to a peer CNDRA lacking NGN-PS support, and will not be processed as intended.

Diagnostic Information:
Collect the following before contacting Oracle Support:

- Event history on active SO server.
- Software release information of dra-Worker's on the dra-Worker server.

1. Recovery

- Potential causes of this alarm are:
  - Routing configuration is incorrect.
  - Peer **CNDRA** has not yet been upgraded.
  - Peer **CNDRA** has not yet operationally enabled NGN-PS.

8016 - MpP16StateMismatch

Alarm Group:
DIAM

Description:
MP P16 Support administrative and operational state mismatch.

Severity:
Major

Instance:
<MP Name>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
eagleXgDiameterMpP16StateMismatch

Cause:
The administrative state of P16 support is not aligned with the operational state.

Diagnostic Information:
Collect the following before contacting Oracle Support:

- Screenshot of active SO server.
- Event History on active SO server.

1. Recovery

1. Potential causes of this alarm are:
   - An MP restart is required.
   - If the 16 Priority Support is mistakenly activated, disable the feature to clear the alarm and align the operational state with administrative state.
   - If the 16 Priority Support is mistakenly de-activated, enable the feature to clear the alarm and align the operational state with administrative state.
2. Alarm clears when the administrative and operational states are aligned.

8017 - MpTaskCpuCongested

Alarm Group
DIAM

Description
DraWorker Task CPU utilization threshold crossed

Severity
Minor, Major, Critical

Instance
Task Name

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpTaskCpuCongested

1. Recovery

- Potential causes of this alarm are:
  - One or more peers are generating more traffic than is nominally expected
  - Configuration requires more CPU for message processing than is nominally expected

8018 - P16MsgMisrouted

Alarm Group
DIAM

Description
16 priority message routed to peer CNDRA lacking 16 priority support

Severity
Major

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterP16MsgMisrouted

1. Recovery

- Potential causes of this alarm are:
  - Peer CNDRA has not yet been upgraded.
  - Peer CNDRA has not yet operationally enabled 16 priority support.

8019 - MpAnswerPriorityModeMismatch

Alarm Group
DIAM

Description
DraWorker Answer Priority Mode administrative and operational state mismatch.

Severity
Major

Instance
<DraWorker Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpAnswerPriorityModeMismatch

1. Recovery

- Potential causes of this alarm are:
  - A DraWorker restart is required.

8020 - MpRoutingThreadPoolStateMismatch

Alarm Group
DIAM

Description
Routing Thread Pool administrative and operational state mismatch.

Severity
Minor

Instance
<DraWorker Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRoutingThreadPoolStateMismatch

1. Recovery

- This alarm is potentially caused when a DraWorker restart is required.

  The alarm clears when administrative and operational states are aligned.

8100 - NormMsgMisrouted

Alarm Group:
DIAG

Description:
Normal message routed onto diagnostic connection.

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
30 (after last occurrence)

OID:
eagleXgDiameterNormMsgMisrouted

1. Recovery:

1. The alarm is potentially caused by a diameter routing misconfiguration.
2. If the problem persists, it is recommended to contact My Oracle Support.

8101 - DiagMsgMisrouted

Alarm Group:
DIAG

Description:
Diagnostic message routed onto normal connection.

Severity:
Minor

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
30 (after last occurrence)

OID:
eagleXgDiameterDiagMsgMisrouted

1. Recovery:

1. The alarm is potentially caused by a diameter routing misconfiguration.
2. If the problem persists, it is recommended to contact My Oracle Support.

8200 - MpRadiusMsgPoolCongested

Alarm Group
DIAM

Description
DA-MP RADIUS message pool utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
MpRadiusMsgPool, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRadiusMsgPoolCongested

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. **MP** server status can be monitored from the **Status & Manage**, and then **Server** page.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each **MP** can be monitored from the **Status & Manage**, and then **KPIs** page. Each **MP** in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each **MP** can be monitored from the **Status & Manage**, and then **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined using the Alarms & Events page.
5. If the problem persists, it is recommended to contact My Oracle Support.

8201 - RclRxTaskQueueCongested

Alarm Group
DIAM

Description
RCL ingress task message queue utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
RclRxTaskQueue, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclRxTaskQueueCongested

1. Recovery:

1. The alarm will clear when the RCL ingress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8202 - RclItrPoolCongested

Alarm Group
DIAM

Description
RCL ITR pool utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
RclItrPool, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclItrPoolCongested

1. Recovery:

1. Adjust the RADIUS **Cached Response Duration** option of the associated Connection configuration set(s) to reduce the lifetime of cached transactions, if needed.
2. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage**, and then **Server** page.
3. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
4. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
5. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined from the Alarms & Events page.
6. If the problem persists, it is recommended to contact My Oracle Support.

8203 - RclTxTaskQueueCongested

Alarm Group
DIAM

Description
RCL egress task threshold crossed.

Severity
Minor, Major, Critical

Instance
RclTxTaskQueue, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclTxTaskQueueCongested

1. Recovery:

1. The alarm will clear when the RCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

8204 - RclEtrPoolCongested

Alarm Group
DIAM

Description
RCL ETR pool utilization threshold crossed.

Severity
Minor, Major, Critical

Instance
RclEtrPool, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRclEtrPoolCongested

1. Recovery:

1. Adjust the RADIUS **Cached Response Duration** option of the associated Connection configuration set(s) to reduce the lifetime of cached transactions, if needed.
2. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site. MP server status can be monitored from the **Status & Manage**, and then **Server** page.
3. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. The ingress traffic rate of each **MP** can be monitored from the **Status & Manage**, and then **KPIs** page. Each MP in the server site should be receiving approximately the same ingress transaction per second.
4. There may be an insufficient number of MPs configured to handle the network traffic load. The ingress traffic rate of each MP can be monitored from the **Status & Manage**, and then **KPIs** page. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.

5. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. The alarm log should be examined from the Alarms & Events page.
6. If the problem persists, it is recommended to contact My Oracle Support.

8205 - RadiusXactionFail

Alarm Group
DIAM

Description
RADIUS connection transaction failure threshold crossed. The presence of this alarm indicates that the server is not responding to requests in a timely manner. A response that is not received in a timely manner constitutes a transaction failure.

Severity
Minor, Major

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterRadiusXactionFail

1. Recovery:

1. Check whether there is an IP network problem, RADIUS server congestion resulting in large response times, or whether a RADIUS server failure has occurred.
2. The user may choose to Admin Disable the corresponding transport connection which will prevent the **DSR** from selecting that connection for message routing, until the cause of the alarm is determined.

8206 - MpRxRadiusAllLen

Alarm Group
DIAM

Description
RADIUS average ingress message length threshold crossed.

Severity
Minor, Major

Instance
MpRxRadiusAllLen, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRxRadiusAllLen

1. Recovery:

1. Investigate traffic sources. One or more peers is sending larger messages than is nominally expected.
2. Adjust the message length thresholds if necessary.

8207 - MpRadiusKeyError

Alarm Group
DIAM

Description
DA-MP RADIUS key error. This alarm is unexpected during normal processing. The presence of this alarm indicates DSR encountered an error while accessing RADIUS encryption keys used to decrypt RADIUS shared secrets.

Severity
Critical

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRadiusKeyError

1. Recovery:

1. Synchronize the RADIUS key file.
2. Restart the DSR process. If the required keys are now available, the alarm is not raised.
3. If the problem persists, it is recommended to contact My Oracle Support.

22001 - Message Decoding Failure

Event Type:
DIAM

Description:
A message received from a peer was rejected because of a decoding failure. Decoding failures can include missing mandatory parameters.

Severity:
Info

Instance:
<TransConnName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterIngressMsgRejectedDecodingFailureNotify

1. Recovery:

- During Diameter Request decoding, the message content was inconsistent with the "Message Length" in the message header. This protocol violation can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

22002 - Peer Routing Rules with Same Priority

Event Type:
DIAM

Description:
A peer routing table search with a received Request message found more than one highest priority Peer Routing Rule match. The system selected the first rule found but it is not guaranteed that the same rule will be selected in the future. It is recommended that Peer Routing Rules be unique for the same type of messages to avoid non-deterministic routing results.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterPeerRoutingTableRulesSamePriorityNotify

1. Recovery:

- Modify one of the Peer Routing Rule Priorities.

22003 - Application ID Mismatch with Peer

Event Type:
DIAM

Description:
While attempting to route a request message to a peer, a peer's transport connection was bypassed because the peer did not support the Application ID for that transport connection.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterApplicationIdMismatchWithPeerNotify

1. Recovery:

1. The system's peer routing table may be using a Route List containing a peer which does not support the Application ID or the list of Application IDs supported by the peer on each connection may not be the same. View the list of Application IDs that the peer supports on each connection and if the Application IDs are not the same for each connection (but should be), the Application ID for any connection can be refreshed by disabling or enabling the connection.
2. The Diameter Node which originated the message (identified by the Origin-Host AVP) could be configured incorrectly and the application is trying to address a node which doesn't support the Application ID. This cannot be fixed using this application.
3. If the problem persists, contact My Oracle Support.

22004 - Maximum pending transactions allowed exceeded

Event Type:
DIAM

Description:
Routing attempted to select an egress transport connection to forward a message but the maximum number of allowed pending transactions queued on the connection has been reached.

Severity:
Info

Instance:
<TransConnName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMaxPendingTxnsPerConnExceededNotify

1. Recovery:

- The maximum number of pending transactions for each connection is set to a system-wide default value. If this event is occurring frequently enough for a particular connection then the maximum value may need to be increased. It is recommended to contact My Oracle Support for assistance.

22005 - No peer routing rule found

Event Type:
DIAM

Description:
A message not addressed to a peer (either Destination-Host AVP was absent or Destination-Host AVP was present but was not a peer's FQDN) could not be routed because no Peer Routing Rules matched the message.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterNoPrtRuleNotify

Cause:
Ingress-request message from a downstream peer is rejected by a Local Node when no peer-routing rules are found in the Peer Routing Table (PRT) and one of the following is true:

- The ingress-request message did not contain a Destination-Host AVP or
- The ingress-request message contained a Destination-Host AVP but did not match with any configured peer node's FQDN or
- Destination-Realm AVP value and the Application-ID in the request message header did not match with configured Realm/Application-Id in Realm Route Table

The Realm Route Table (table RealmRoute) managed object is used to perform message routing based upon the Destination-Realm and Application-ID in a request message. The Realm Route Table is dynamically configured on the active Overseer.

Diagnostic Information:
Analyze the event history and event #22005 which will have following information regarding the failure diameter message:

- `<TransConnName>` (Receiving connection)
- `<PeerName>` (Name of the receiving peer)
- `<DestRealm>` (Value found in Request message Destination-Realm AVP)
- `<ApplicationID>` (Application ID in the Request message)
- `<DestHostFQDN>` (FQDN found in request message Destination-Host AVP, if present)
- `<OriginHostFQDN>` (FQDN found in request message Origin-Host AVP)

The Diameter Ingress Transaction Exception group measurement report contains the RxNoRulesFailure (10034) measurement, which is also pegged in the same scenario.

1. Recovery:

1. Either the message was incorrectly routed to this node or additional Peer Routing Rules need to be added. View and update the Peer Routing Rules.
2. If multiple peer routing tables are used, ensure the correct table is applied for the message in question.
3. If the problem persists, it is recommended to contact My Oracle Support.

22007 - Inconsistent Application ID Lists from a Peer

Event Type:
DIAM

Description:
The list of Application IDs supported by a peer during the Diameter Capabilities Exchange procedure on a particular transport connection is not identical to one of the list of Application IDs received from the peer over a different available transport connection to that peer.

Severity:
Info

Instance:
<PeerName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterSupportedAppIdsInconsistentNotify

1. Recovery:

1. A peer with multiple transport connections has established a connection and provided a list of supported Application IDs which does match a previously established connection. This could prevent Request messages from being routed uniformly over the peer's transport connections because the decision to route a message containing an Application ID is based upon the list of Application IDs supported on each transport connection. View the list of Application IDs that the peer supports on each connection and if the Application IDs are not the same for each connection (but should be), the Application ID for any connection can be refreshed by disabling or enabling the connection.
2. If the problem persists, it is recommended to contact My Oracle Support.

22008 - Orphan Answer Response Received

Event Type:
DIAM

Description:
An answer response was received for which no pending request transaction existed, resulting in the answer message being discarded. When a Request message is forwarded the system saves a pending transaction, which contains the routing information for the answer response. The pending transaction is abandoned if an answer response is not received in a timely fashion.

Severity:
Info

Instance:
<TransConnName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterOrphanAnswerResponseReceivedNotify

Cause:
An answer message is received without any corresponding pending transaction. The message is discarded.

Diagnostic Information:
Reasons the pending transaction is not available include:

- Peer CNDRA's Tx sender buffer is filling up causing connection congestion.
- PAT expiry or total transaction life-time expiry is causing transaction timeout.

The associated measurement tag for this event is RxAnswerUnexpected (10008), which is the number of times that the DRL receives an answer message event from DCL/RCL with a valid Connection ID for which a pending transaction cannot be found.

1. Recovery:

- If this event is occurring frequently, the transaction timers may be set too low.

22009 - Application Routing Rules with Same Priority

Event Type:
DIAM

Description:
An application routing table search with a received Request message found more than one highest priority application routing rule match. At least two application routing rules with the same priority matched an ingress Request message. The system selected the first application routing rule found.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterApplicationRoutingTableRulesSamePriorityNotify

1. Recovery:
1. It is recommended that application routing rules be unique for the same type of messages to avoid unexpected routing results.
2. If the problem persists, it is recommended to contact My Oracle Support.

22010 - Specified DAS Route List not provisioned

Event Type:
DIAM

Description:
The DAS Route List specified by the message copy trigger point is not provisioned.

Severity:
Info

Instance:
<RouteListId>

HA Score:
Normal

Throttle Seconds:
10

> **Note:**
>
> Because many route lists can be created on a DraWorker server, care must be taken to prevent excessive event generation with these resources.

OID:
eagleXgDiameterSpecifiedDasRouteListNotProvisionedNotify

1. Recovery:

1. Provisioning is incorrect/misconfigured. Verify provisioning and provision/correct provisioning.
2. If this problem persists, it is recommended to contact My Oracle Support for assistance.

22012 - Specified MCCS not provisioned

Event Type:
DIAM

Description:
The Message Copy Config Set specified by the trigger point is not provisioned.

Severity:
Info

Instance:
<MCCS>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterSpecifiedMCCSNotProvisionedNotify

1. Recovery:

1. Verify the configured value of MCCS with the trigger point.
2. Verify the Message Copy CfgSet (MCCS) provisioning is properly configured.
3. If the problem persists, it is recommended to contact My Oracle Support.

22013 - DAS Peer Number of Retransmits Exceeded for Copy

Event Type:
DIAM

Description:
The configured number of **Message Copy** retransmits has been exceeded for the DAS Peer.

Severity:
Info

Instance:
<MCCS>

HA Score:
Normal

Throttle Seconds:
10

> **Note:**
>
> Because many route lists can be created on a DraWorker server, care must be taken to prevent excessive event generation with these resources.

OID:
eagleXgDiameterNumberOfRetransmitsExceededToDasNotify

1. Recovery:
1. Verify the configured value of 'Max Retransmission Attempts'
2. Verify local provisioning to connections to intended DAS peer server(s) are in service and no network issues in path(s) to intended DAS peer server(s) exist.
3. Verify DAS peer provisioning to insure proper configuration.
4. If the problem persists, it is recommended to contact My Oracle Support for assistance.

22014 - No DAS Route List specified

Alarm Group:
DIAM

Description:
No valid DAS Route List was specified in the Message Copy Config Set.

Severity:
Info

Instance:
<RouteListId>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterNoDasRouteListSpecifiedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for further assistance.

22016 - Peer Node Alarm Aggregation Threshold

Alarm Group:
DIAM

Description:
This alarm occurs when there are a critical number of peer node alarms for a single network element and it exceeds the configurable alarm threshold.

> **Note:**
>
> The alarm thresholds are configurable using the Alarm Threshold Options tab on **Diameter**, and then **Configuration**, and then **System Options**.

When this alarm is generated, the system clears all individual peer node alarms (alarm 22051) for the peer node.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPeerNodeUnavailableThresholdReachedNotify

Cause:
The number of critical peer node alarms for a single network element exceeds the configurable alarm threshold.

Diagnostic Information:
Refer to Alarm 22051- Peer Unavailable. When this alarm is reported, the system clears all the individual peer node alarms (alarm 22051) for the peer node.

1. Recovery:

1. Check the peer status.
2. Verify IP network connectivity exists between the MP server and the peer node.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify the peer is not under maintenance.
5. It is recommended to contact My Oracle Support for assistance.

22017 - Route List Alarm Aggregation Threshold

Alarm Group:
DIAM

Description:
This alarm occurs when there are a ‘Critical’ number of Route List alarms for the Network Element.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRouteListUnavailableThresholdReachedNotify

Cause:
The alarm # 22017 raises when the total number of Route List alarms for a single NE have reached the configured Route List Failure Critical Aggregation Alarm Threshold.

The alarm gets cleared when the total number of Route List alarms for a single NE have dropped to at least 20% below the configured Route List Failure Critical Aggregation Alarm Threshold.

Diagnostic Information:
For further information on this alarm:

1. Examine the alarm log on Active Overseer Server.
2. Find all the route lists with a problem for the specific MP.
3. A Route List's operational status is always set to the operational status of the Route Group within the Route List that is designated as the Active Route Group.
4. If all Route Groups within the route list are Unavailable, then the Route List is Unavailable and there is no Active Route Group.

1. Recovery:

1. View the Route List to monitor Route List status.
2. Verify that IP network connectivity exists between the MP server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify that the peers in the Route List are not under maintenance.
5. It is recommended to contact My Oracle Support for assistance.

22018 - Maintenance Leader HA Notification to go Active

Alarm Group:
DIAM

Description:
This alarm occurs when a DraWorker has received a notification from HA that the Maintenance Leader resource should transition to the Active role.

Severity:
Info

Instance:
<MP Node ID>

HA Score:
Normal

Throttle Seconds:
1

OID:
eagleXgDiameterDaMpLeaderGoActiveNotificationNotify

1. Recovery:

- No action necessary.

22019 - Maintenance Leader HA Notification to go OOS

Alarm Group:
DIAM

Description:
This alarm occurs when a DraWorker has received a notification from HA that the Maintenance Leader resource should transition to the OOS role.

Instance:
<MP Node ID>

Severity:
Info

HA Score:
Normal

Throttle Seconds:
1

OID:
eagleXgDiameterDaMpLeaderGoOOSNotificationNotify

1. Recovery:

- No action necessary.

22020 - Copy Message size exceeded the system configured size limit

Event Type:
DIAM

Description:
The generated Copy message size exceeded the max message size on the system.

Severity:
Info

Instance:
<DraWorker>

HA Score:
Normal

Throttle Seconds:
10

> **Note:**
>
> Because many copy messages can exceed the system configured size, care must be taken to prevent excessive generation with these resources.

OID:
eagleXgDiameterCopyMessageSizeExceededNotify

1. Recovery:
1. Verify the size of the Request and Answer messages and see it exceeds the system set message size.
2. Review provisioning and correct provisioning and see whether answers also needed to copy.

   Requests and answers may be copied to DAS.
3. If this problem persists, it is recommended to contact My Oracle Support for assistance.

22021 - Debug Routing Info AVP Enabled

Alarm Group:
DIAM

Description:
Debug Routing Info AVP is enabled.

Severity:
Minor

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDebugRoutingInfoAvpEnabledNotify

1. Recovery:

1. Change the `IncludeRoutingInfoAvp` parameter to *no* in the DpiOption table on the NO for a 2-tier system or on the SO for a 3-tier system.
2. If the problem persists, it is recommended to contact My Oracle Support.

22022 - Forwarding Loop Detected

Alarm Group:
DIAM

Description:
Ingress Request message received was previously processed by the local node as determined from the Route-Record AVPs received in the message.

Severity:
Major

Instance:
<Peer Name>

HA Score:
Normal

Auto Clear Seconds:
30

OID:
eagleXgDiameterForwardingLoopDetectedNotify

1. Recovery:

1. An ingress request message was rejected because message looping was detected. In general, the forwarding node should not send a message to a peer that has already processed the message (it should examine the Route-Record AVPs before message forwarding). If this type of error is occurring frequently, then the forwarding node is most likely mis-routing the message. This should not be related to a configuration error because the identity of the local node is sent to the peer during the Diameter Capabilities Exchange procedure when the Connection comes into service.
2. If Path Topology Hiding is activated and Protected Network Node's Route-Records are obscured with PseudoNodeFQDN, then inter-network ingress message loop detection could reject the message if same Request message is routed back to

DEA. If this type of error is occurring then the forwarding node is most likely mis-routing the message back to DEA.

3. If the problem persists, it is recommended to contact My Oracle Support.

22051 - Peer Unavailable

Alarm Group:
DIAM

Description:
Unable to access the Diameter Peer because all of the transport connections are down. Peer node unavailability can happen in these cases:

- All connections toward a peer are no longer candidates for routing Request messages.
- No available connections within the peer node support the Application ID. This is functionally equivalent to the peer node being unavailable.
- The Connection Priority Level (CPL) value for a resource is changed to 99, which means the operational status is Unavailable. The CPL value of a connection can be found in the active SO.
- The number of established connections drops below the configured Minimum Connection Capacity.

Severity:
Critical

Instance:
<PeerName> (of the Peer which failed).

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPeerUnavailableNotify

Cause
The Alarm #22051 raises when the Diameter Peer is not accessible as all the transport connections are down.

Diagnostic Information
Peer node is unavailable in the following cases:

- All connections towards a peer are no longer candidates for routing Request messages.
- No available connections within the peer node support the Application ID. This is functionally equivalent to the peer node being unavailable.
- The Connection Priority Level (CPL) value for a resource is changed to 99, which means the operational status is Unavailable. The CPL value of a connection can be found in the active SO.

- The number of established connections drops below the configured Minimum Connection Capacity.

1. Recovery:
1. Confirm a connection is provisioned for the peer node.
   - Verify IP network connectivity exists between the MP server and the peer nodes using ping, traceroute, or other means.
   - Examine the event history logs for additional DIAM events or alarms from the MP server.
   - Verify the peer is not under maintenance.
   - Verify there are connections provisioned for the peer node.
   - Verify the status of all connections toward the peer node.
     View the Transaction Configuration Set of the peer node.

     If the peer node has a corresponding Transaction Configuration Set setting, then confirm the Application ID is supported.
2. Confirm the peer node supports the Application ID in the request message.
3. Resolve any congestion issues on the peer node.
4. If the problem persists, it is recommended to contact My Oracle Support.

22052 - Peer Degraded

Alarm Group:
DIAM

Description:
The peer has some available connections, but less than its minimum connection capacity. Continued routing to this peer may cause congestion or other overload conditions.

Severity:
Major

Instance:
<PeerName> (of the Peer which is degraded)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPeerDegradedNotify

Cause:

- If the number of available connections to peer node is less than minimum connection capacity which is default 1 per Peer Node, then Peer Node Status will be degraded, and alarm 22052 raises.

- If all the connections are degraded for the peer node, then Peer Node status will be degraded and Alarm 22052 raises.

Diagnostic Information:

- Verify the number of available connection to that peer should be greater than minimum connection capacity which is default 1.
- Peer CNDRA configurations on active SO
- Savelogs on active SO
- Event History on active SO

1. Recovery:

1. Check the Peer status.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs for additional DIAM events or alarms from this MP server.
4. Verify the peer is not under maintenance.
5. Make sure the number of available connections to that peer node is greater than minimum connection capacity configured.
6. If the problem persists, it is recommended to contact My Oracle Support.

22053 - Route List Unavailable

Alarm Group:
DIAM

Description:
All route groups with the route list are unavailable. A Route List becomes unavailable when all of its peers become unavailable and a peer becomes unavailable when all of its transport connections become unavailable.
If a Transport Connection is configured for Initiate mode, the network element periodically attempts to recover the connection automatically if its Admin State is enabled. If the Transport Connection is configured for Responder-Only mode, the peer is responsible for re-establishing the transport connection.
Examine the Event history and software release information for the route groups.

Severity:
Critical

Instance:
<RouteListName> (of the Route List which failed)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRouteListUnavailableNotify

Cause:
All route groups within the route list are unavailable. Check the Route list status.

Diagnostic Information
Examine the following for the route groups:

- Event history
- Software release information

1. Recovery:

1. Check the Route List status.
2. Verify IP network connectivity exists between the **MP** server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this **MP** server.
4. Verify the peers in the route list not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support.

22054 - Route List Degraded

Alarm Group:
DIAM

Description:
The Route List's Operational Status has changed to degraded because the capacity of the Route List's active route group has dropped below the Route List's configured minimum capacity. There are two potential causes:

1. One or more of the Route List's peers become Unavailable. A peer becomes unavailable when all of its transport connections become unavailable. If a transport connection is configured for Initiate mode, the network element periodically attempts to recover the connection if its admin state is enabled. If the transport connection is configured for responder-only mode, the peer is responsible for re-establishing the transport connection.
2. The Route Groups within the Route List may not have been configured with sufficient capacity to meet the Route List's configured minimum capacity.

Severity:
Major

Instance:
<RouteListName> (of the Route List which is degraded)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRouteListDegradedNotify

Cause:
There are no available Route Groups, and the Operational Status of one or more Route Groups within the Route List is degraded.

Diagnostic Information:
A Route List's operational status is always set to the operational status of the Route Group within the Route List that is designated as the Active Route Group.
DRL determines which Route Group within a Route List is designated the Active Route Group for that Route List as follows:

- If the operational status of one or more Route Groups within the Route List is Available, then the Active Route Group for the Route List is the Available Route Group with the highest priority
- If there are no Available Route Groups, and the operational status of one or more Route Groups within the Route List is Degraded, the Active Route Group is the Degraded Route Group with the highest Current Capacity. If two or more degraded Route Groups exist with equal Current Capacity, then the Active Route Group is the one with the highest Priority
- If all Route Groups within the route list are Unavailable, then the Route List is Unavailable and there is no Active Route Group

1. Recovery:

1. Verify Route List status and configured minimum capacity.
2. Verify IP network connectivity exists between the **MP** server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this **MP** server.
4. Verify the peers in the Route List are not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support.

22055 - Non-Preferred Route Group in Use

Alarm Group:
DIAM

Description:
The application has started to utilize a Route Group other than the highest priority Route Group to route Request messages for a Route List because the highest priority Route Group specified for that Route List has either become Unavailable or its capacity has dropped below the minimum capacity configured for the Route List while a lower priority Route Group has more capacity.

The preferred Route Group (i.e., with highest priority) is demoted from the Active Route Group to a Standby Route Group when a peer failure occurs causing the Route Group's Operational Status to change to Unavailable or Degraded. A Route Group becomes Degraded when its capacity has dropped below Route List's configured minimum capacity. A Route Group becomes Unavailable when all of its peers have an Operational Status of Unavailable or Degraded.

A Peer becomes Unavailable when all of its transport connections become Unavailable. If a Transport Connection is configured for Initiate mode, the Network Element will periodically attempt to automatically recover the connection if its Admin

State is Enabled. If the Transport Connection is configured for Responder-Only mode, the peer will be responsible for re-establishing the transport connection.

Severity:
Minor

Instance:
<RouteListName> (of the concerned Route List)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterNonPreferredRouteGroupInUseNotify

1. Recovery:

1. Check the Route List status and configured minimum capacity.
2. Verify that IP network connectivity exists between the **MP** server and the peers.
3. Check the event history logs for additional DIAM events or alarms from this **MP** server.
4. Verify that the adjacent server is not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support.

22056 - Connection Admin State Inconsistency Exists

Alarm Group:
DIAM

Description:
An operator request to change the Admin State of a transport connection was not completely processed due to an internal error. The admin state is either disabled from an egress routing perspective but the connection could not be taken out of service or the admin state is enabled from an egress routing perspective but the connection is not in service.

Severity:
Major

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnAdminStateInconsistencyNotify

1. Recovery:

1. If the transport connection's Admin State is Disabled but the transport connection was not taken out of service due to an internal error do the following actions to correct the failure:
   a. Enable the connection.
   b. Wait for this alarm to clear.
   c. Disable the connection.
2. If the transport connection's Admin State is Enabled but the transport connection was not taken out of service due to an internal error do the following actions to correct the failure:
   a. Disable the connection.
   b. Wait for this alarm to clear.
   c. Enable the connection.
3. If the problem persists, it is recommended to contact My Oracle Support.

22057 - ETG Rate Limit Degraded

Alarm Group:
DIAM

Description:
The ETG Rate Limit has exceeded the defined threshold.

Severity:
Major

Instance:
<ETGName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgRateLimitDegradedNotify

Cause:
This alarm triggers when Rate Limiting is Enabled through active SO server menu, **Diameter > Maintenance > Egress Throttle Groups**.

- Rate Limiting Operational Status transitions from Available to Degraded.
- Rate Limiting Operational Status transitions from Inactive to Degraded.

Diagnostic Information

- Screen snapshot of active SO server through menu, **Main Menu> Diameter -> Maintenance -> Egress Throttle Groups**.
- Savelogs of all MPs.
- DSR logs of all MPs.

- Export DSR configuration on active SO server.

1. Recovery:

1. Check the configuration in **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups** and **Diameter**, and then **Maintenance**, and then **Connections** to determine if the sending Peers/Connections are offering too much traffic.
3. If the problem persists, collect the logs list in Diagnostic information and it is recommended to contact My Oracle Support.

22058 - ETG Pending Transaction Limit Degraded

Alarm Group:
DIAM

Description:
The ETG Pending Transactions Limit has exceeded the defined threshold.

Severity:
Major

Instance:
<ETGName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgPendingTransLimitDegradedNotify

Cause:
When Pending Transaction limiting is Enabled through Active SO, menu **Diameter -> Maintenance -> Egress Throttle Groups**, the alarm will be triggered when the following conditions met:

- Pending Transaction Limiting Operational Status transitions from Available to Degraded
- Pending Transaction Limiting Operational Status transitions from Inactive to Degraded

Diagnostic Information:

- Screen Snapshot of active SO via menu: **Main Menu > Diameter > Maintenance > Egress Throttle Groups** .
- Savelogs of all MPs.
- DSR logs of all MPs.

- Export DSR configuration.

1. Recovery:

1. Check the configuration in **Diameter**, and then **Configuration**, and then **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups** and **Main Menu**, and then **Diameter**, and then **Maintenance**, and then **Connections** to determine if the sending Peers/Connections are offering too much traffic.
3. Determine if the receiving Peers or Connections in the ETG are not responding with Answers in a timely manner because they are either busy or overloaded.
4. If the problem persists, collect logs in Diagnostic information and it is recommended to contact My Oracle Support.

22059 - Egress Throttle Group Message Rate Congestion Level changed

Event Group:
DIAM

Description:
The Egress Throttle Group Message rate Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity:
Info

Instance:
<ETGName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterEtgRateCongestionNotify

1. Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Diameter**, and then **Configuration**, and then **Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups** and/or **Diameter**, and then **Maintenance**, and then **Connections**
3. Typically all routes to a server should be in an ETG. However, if that is not the case, alternate routes may be out of service and could cause overloading of traffic towards connections contained in this ETG. Evaluate traffic distribution to server connections and see if any alternate routes to server are unavailable causing overloading of traffic on an ETG.
4. It is recommended to contact My Oracle Support for assistance.

22060 - Egress Throttle Group Pending Transaction Limit Congestion Level changed

Event Group:
DIAM

Description:
The Egress Throttle Group Pending Transaction Limit Congestion Level has changed. This will change the Request priority that can be routed on peers and connections in the ETG.

Severity:
Info

Instance:
<ETGName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterEtgPendingTransCongestionNotify

1. Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Diameter**, and then **Configuration**, and then **Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Diameter**, and then **Maintenance**, and then **Egress Throttle Groups** and/or **Diameter**, and then **Maintenance**, and then **Connections**
3. Typically all routes to a server should be in a ETG, however if that is not the case, then those routes becoming out of service could cause overloading of traffic towards connections contained in this ETG. Evaluate traffic distribution to server connections and see if any alternate routes to server are unavailable causing overloading of traffic on an ETG.
4. The receiving Peers or Connections in the ETG are not responding with Answers in a timely manner. Check to see if they are busy or overloaded.
5. If the problem persists, it is recommended to contact My Oracle Support for assistance.

22061 - Egress Throttle Group Monitoring stopped

Alarm Group:
DIAM

Description:
ETG Rate and Pending Transaction Monitoring is stopped on all configured ETGs

Severity:
Minor

Instance:
<DA-MP Hostname>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgMonitoringStoppedNotify

1. Recovery:

1. Verify ComAgent links setup between DA-MPs have not gone OOS causing SMS Service to not receive Responses from DA-MP Leader under **Communication Agent**, and then **Maintenance**.
2. Verify ComAgent links are established between DA-MPs under **Communication Agent**, and then **Maintenance**
3. Verify the No-MP Leader condition in **Diameter**, and then **Maintenance**, and then **DA-MPs**, and then **Peer DA-MP Status** that at least 1 DA-MP is MP-Leader.
4. If the problem persists, it is recommended to contact My Oracle Support.

22062 - Actual Host Name cannot be determined for Topology Hiding

Event Group:
Diameter

Description:
Topology Hiding could not be applied because the Actual Host Name could not be determined.

Severity:
Info

Instance:
<CfgSetName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTopoHidingActualHostNameNotFoundNotify

1. Recovery:

1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set.

2. If any Peer CNDRA Applications are activated on Peer CNDRA, ensure that any specific Application Level Topology Hiding feature is not conflicting with the contents of Actual Host Names specified in the MME Configuration Set.
3. Check if the first instance of a Session-ID AVP in the Request/Answer message contains the mandatory delimited ";".
4. If the problem persists, it is recommended to contact My Oracle Support.

22063 - Diameter Max Message Size Limit Exceeded

Event Type:
DIAM

Description:
The size of the message encoded by Peer CNDRA has exceeded its max limits.

Severity:
Info

Instance:
<TransConnName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDiameterMaxMsgSizeLimitExceededNotify

1. Recovery:

- No action required. However, if this event is seen to be incrementing consistently, it is recommended to contact My Oracle Support for assistance.

22064 - Upon receiving Redirect Host Notification the Request has not been submitted for re-routing

Event Type:
DIAM

Description:
This event indicates that the Peer CNDRA has encountered a Redirect Host Notification that it can accept for processing but cannot continue processing due to some reason, such as internal resources exhaustion.

Severity:
Info

Instance:
<PeerName>

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterRxRedirectHostNotRoutedNotify

1. Recovery:

1. Examine the DraWorker congestion status and related measurements and take appropriate action.
2. If the problem persists, it is recommended to contact My Oracle Support.

22065 - Upon receiving Redirect Realm Notification the Request has not been submitted for re-routing

Event Type:
DIAM

Description:
The Redirect Realm Notification received is accepted but cannot be processed due to some reason, such as internal resources exhaustion.

Severity:
Info

Instance:
<PeerName>

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterRxRedirectRealmNotRoutedNotify

1. Recovery:

1. Examine the DraWorker congestion status and related measurements and take appropriate action.
2. If the problem persists, it is recommended to contact My Oracle Support.

22066 - ETG-ETL Scope Inconsistency

Alarm Group:
DIAM

Description:
An ETG's Control Scope is set to ETL, but the ETG is not configured against an ETL.

Severity:
Minor

Instance:
<ETG Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgEtlScopeInconsistencyNotify

1. Recovery:

1. Correct the configuration inconsistency by changing the Control Scope of the ETG from ETL to ETG, or by adding the ETG to an ETL.
2. If a backup image has been restored to the SOAM, but not the NOAM, restoring a consistent backup image for the NOAM should resolve the problem.
3. If the problem persists, it is recommended to contact My Oracle Support.

22067 - ETL-ETG Invalid Association

Event Type:
DIAM

Description:
An ETL is associated with an ETG that does not exist.

Severity:
Minor

Instance:
<ETL Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterEtgEtlInvalidAssocNotify

1. Recovery:

1. Correct the configuration inconsistency by updating the ETL to refer to a valid ETG, or by installing consistent backups on the NOAM and SOAM.
2. If the problem persists, it is recommended to contact My Oracle Support.

22068 - TtpEvDoicException

22068 - 001 - TtpEvDoicException: DOIC OC-Supported-Features AVP not received

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:001

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- The Peer Node associated with the TTP is not responding to a DOIC Capability Announcement (DCA). This can occur when the Peer Node either does not support DOIC or DOIC has been disabled on the Peer Node. The operator should either disable DOIC on the DSR associated with TTP by setting the TTP's "Dynamic Throttling Admin State" to Disabled or enable DOIC on the Peer Node.

22068 - 002 - TtpEvDoicException: DOIC OC-Feature-Vector AVP contains an invalid value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:002

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- The Peer Node associated with the TTP has selected a DOIC Abatement Algorithm not supported by the TTP. This should never happen and may be the result of a mis-configuration or bug on the Peer Node. If this error persists, the operator should disable DOIC for the TTP by setting the TTP's "Dynamic Throttling Admin State" to Disabled or enable DOIC on the Peer Node.

22068 - 003 - TtpEvDoicException: DOIC OC-Report-Type AVP contains an unsupported value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:003

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- The Peer Node associated with the TTP is sending a DOIC overload report which is not supported by DSR at this time. The operator should disable Realm-based DOIC overload reports on the Peer Node.

22068 - 004 - TtpEvDoicException: DOIC OC-Sequence-Number AVP contains an out of order sequence number

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:004

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- The Peer Node associated with the TTP has sent a DOIC overload report that is out of sequence. If this error occurs infrequently, then it may have been caused by a timing delay whereby Answer messages received from the Peer Node were delivered out of order. If this error occurs frequently, then the Peer Node may be in violation of the DOIC specification.

22068 - 005 - TtpEvDoicException: DOIC OC-Reduction-Percentage AVP contains an invalid value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:005

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- The Peer Node associated with the TTP has sent a DOIC overload report containing an OC-Reduction-Percentage AVP value greater than 100. If this error occurs infrequently, then there may be a DOIC software error in the Peer Node. If this error occurs frequently, then the error may be caused by a Peer Node DOIC mis-configuration problem.

22068 - 006 - TtpEvDoicException: DOIC OC-Validity-Duration AVP contains an invalid value

Event Type:
DIAM

Description:
DOIC Protocol Error

Severity:
Info

Instance:
<TTP Name>:006

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- The Peer Node associated with the TTP has sent a DOIC overload report containing an OC-Validity-Duration AVP value greater than the maximum allowed. The maximum value for the OC-Validity-Duration AVP is 86,400 seconds (24 hours). If this error occurs infrequently, then there may be a DOIC software error in the Peer Node. If this error occurs frequently, then the error may be caused by a Peer Node DOIC mis-configuration problem.

22069 - TtpEvDoicOlr

22069 - 001 - TtpEvDoicOlr: Valid DOIC OLR Applied to TTP

Event Type:
DIAM

Description:
A DOIC OverLoad Request (OLR) was received from a Peer Node and applied to a configured TTP.

Severity:
Info

Instance:
<TTP Name>:001

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- No action required.

22070 - TtpEvDegraded

22070 - 001 - TtpEvDegraded: TTP Degraded, Peer Overload

Event Type:
DIAM

Description:
TTP Degraded

Severity:
Info

Instance:
<TTP Name>:001

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDegradedNotify

1. Recovery:

- No action required.

22070 - 002 - TtpEvDegraded: TTP Degraded, Peer Overload Recovery

Event Type:
DIAM

Description:
TTP Degraded

Severity:
Info

Instance:
<TTP Name>:002

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDegradedNotify

1. Recovery:

- No action required.

22070 - 003 - TtpEvDegraded: TTP Degraded, Static Rate Limit Exceeded

Event Type:
DIAM

Description:
TTP Degraded

Severity:
Info

Instance:
<TTP Name>:003

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDegradedNotify

1. Recovery:

- No action required.

22071 - TtgEvLossChg

22071 - 001 - TtgEvLossChg: TTG Loss Percent Changed

Event Type:
DIAM

Description:
TTG's Loss Percentage was modified.

Severity:
Info

Instance:
<TTG Name>:001

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterTtpEvDoicExceptionNotify

1. Recovery:

- No action required.

22072 - TTP Degraded

Alarm Group
DIAM

Description
The TTP's Operational Status has been changed to Degraded.

Severity
Major

Instance
<TTP Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtpDegradedNotify

1. Recovery

- No action required.

22073 - TTP Throttling Stopped

Alarm Group
DIAM

Description
TTP rate throttling has been suspended due to an internal failure.

Severity
Minor

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtpThrottlingStoppedNotify

1. Recovery:

1. Verify that ComAgent links setup between DA-MPs have not gone OOS causing SMS Service to not receive Responses from DA-MP Leader under **Communication Agent**, and then **Maintenance**.
2. Verify ComAgent links are established between DA-MPs under **Communication Agent**, and then **Maintenance**
3. Verify the No-MP Leader condition in **Diameter**, and then **Maintenance**, and then **DA-MPs**, and then **Peer DA-MP Status** that at least 1 DA-MP is MP-Leader.
4. If the problem persists, it is recommended to contact My Oracle Support.

22074 - TTP Maximum Loss Percentage Threshold Exceeded

Alarm Group
DIAM

Description
The Maximum Loss Percentage Threshold assigned to the TTP has been exceeded.

Severity
Major

Instance
<TTP Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtpMaxLossPercentageExceededNotify

1. Recovery

- No action required.

22075 - Message is not routed to Application

Alarm Group:
DIAM

Description:
ART Rule-X was selected, but message was not routed because Peer CNDRA Application is disabled or not available.

Severity:
Major

Instance:
<Peer CNDRA Application Name>

HA Score:
Normal

Auto Clear Seconds:
0

OID:
eagleXgDiameterArtMatchAppUnavailableNotify

1. Recovery:

1. Check the Application Status and Enable the application if the Admin State of the Peer CNDRA application is Disabled for a particular DraWorker(s) which raised the alarm.
2. If the Application is Enabled for a particular DraWorker, but the Operational Status is Unavailable or Degraded, then refer to the Operational Reason and rectify it accordingly.
3. If the problem persists, it is recommended to contact My Oracle Support.

22076 - TTG Maximum Loss Percentage Threshold Exceeded

Alarm Group
DIAM

Description
The "Maximum Loss Percentage Threshold" assigned to the Route Group within the Route List has been exceeded.

Severity
Major

Instance
<Route List Name>:<Route Group Name>.<TTG Name>

HA Score
Normal

Auto Clear Seconds
0

OID
eagleXgDiameterTtgMaxLossPercentageExceededNotify

1. Recovery

- No action required.

22077 - Excessive Request Reroute Threshold Exceeded

Alarm Group:
DIAM

Description:
Request reroutes due to Answer response and/or Answer timeout having exceeded the configured onset threshold percentage on the DraWorker server.

Severity:
Major

Instance:
MpReroutePercent

HA Score:
Normal

Auto Clear Seconds:
N/A

> **Note:**
>
> The alarm clears when the percentage of Request reroutes due to Answer Result-code matching "Reroute on Answer" and Answer Timeout drops below the configured abatement threshold and remains there for the configured abatement time. The alarm also clears when the Peer CNDRA process is stopped or restarted.

OID:
eagleXgDiameterMpExcessiveRequestRerouteNotify

1. Recovery:

1. This alarm is an indication of reroutes exceeding the configured threshold, due to responses from the Peer Node exceeding the Pending Answer timer in Peer CNDRA or due to configured "Reroute on Answer" Result codes.
2. If rerouting is triggered due to Answer Result-code:
   a. Use measurement TxRerouteAnswerResponse to identify any peer (or set of peers) being identified as triggering reroute.
   b. If a peer (or set of peers) is identified, validate that Reroute-on-Answer is properly configured for that peer.
   c. Check for congestion being reported by the peer.
3. If rerouting is triggered due to Answer Timeout:
   a. Use measurement TxRerouteAnswerTimeout to identify any peer (or set of peers) being identified as timing out.
   b. If a peer (or set of peers) is identified, verify that Pending Answer Timer and Transaction Lifetime are properly configured.
   c. Check for congestion being reported by the peer.

4. If the problem persists, it is recommended to contact My Oracle Support.

22078 - Loop or Maximum Depth Exceeded in ART or PRT Search

Alarm Group:
DIAM

Description:
An ART/PRT search has resulted in either a loop between ART/PRT tables, or the search depth has exceeded the maximum allowed depth.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterNestedArtPrtSearchErrorNotify

1. Recovery:
1. If the error was a search loop, the customer should change at least one of the rules in the search sequence to avoid a loop. If the error was a maximum depth exceeded, the customer should remove one or more rules in the search sequence.
2. If the problem persists, it is recommended to contact My Oracle Support.

22082 - RouteList is not Provisioned in System Options

Alarm Group:

DIAM

Description:

Radius Route List is not provisioned in the system options.

Severity:

Info

Instance:

<MPName>

HA Score:

Normal

Throttle Seconds:

10

OID:

eagleXgDiameterInvalidDestRouteListNotify

1. Recovery

1. If the error was a search loop, the customer should change at least one of the rules in the search sequence to avoid a loop. If the error was a maximum depth exceeded, the customer should remove one or more rules in the search sequence.
2. If the problem persists, it is recommended to contact My Oracle Support.

22101 - Connection Unavailable

Alarm Group:
DIAM

Description:
Connection is unavailable for Diameter Request/Answer exchange with peer.

> **Note:**
>
> This alarm is not raised when the Suppress Connection Unavailable alarm for a Transport Connection is set to Yes.

Alarm 22101 is generated when the connection's administrative state is enabled and the connection is not in a state where it can send or receive Diameter Requests or Answers to/from the peer. The alarm is generated when one of the following occurs.

- Connection's Admin State transitions from disabled to enabled
- Connection's Operational Status transitions from available to unavailable
- Connection's Operational Status transitions from degraded to unavailable

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnectionUnavailableAlarmNotify

Cause:
Alarm #22101 raises when the connection's administrative state is enabled and the connection is not in a state where it can send or receive Diameter Requests or Answers to/from the peer. The alarm is generated when one of the following occurs:

- Connection's Admin State transitions from disabled to enabled
- Connection's Operational Status transitions from available to unavailable
- Connection's Operational Status transitions from degraded to unavailable

Diagnostic Information:
Confirm any of following conditions is occurring:

1. A host IP interface is down
2. A host IP interface is unreachable from the peer
3. A peer IP interface is down
4. A peer IP interface is unreachable from the host

Verify the following are configured and available:

1. Remote IP availability
2. Remote server (port) availability
3. Network availability
4. Local IP route to remove
5. Local MP service availability
6. Configuration correctness, such as CEX parameter matching with remove

1. Recovery:

1. Confirm the host IP interface is down or unreachable from the peer.
2. Confirm the peer IP interface is down or unreachable from the host.
3. Verify the following are configured and available:
   - Remote IP availability
   - Remote server (port) availability
   - Network availability
   - Local IP route to remove
   - Local MP service availability
   - Configuration correctness, such as CEX parameter matching with remove
4. Identify the most recent Connection Unavailable event in the event log for the connection and use the Event's recovery steps to resolve the issue.
5. If the problem persists, it is recommended to contact My Oracle Support.

22102 - Connection Degraded

Alarm Group:
DIAM

Description:
Connection is only available for routing messages with a priority greater than or equal to the connection's congestion level. This alarm is generated when:

- Connection congestion when the Peer CNDRA Tx sender buffer is at maximum capacity
- The connection's administrative state is enabled and the connection is in congestion. Requests and Answers continue to be received and processed from the peer over the connection, and attempts to send Answers to the peer still occur. The alarm is raised when one of the following occurs:
  - Connection's Operational Status transitions from available to degraded (connection has become congested or watchdog algorithm has failed)
  - Connection's Operational Status transitions from unavailable to degraded (connection has successfully completed the capabilities exchange and is performing connection proving)
- Connection egress message rate threshold has been crossed
- Diameter connection is in watchdog proving
- Diameter connection is in graceful disconnect
- Diameter peer signaled the remote is busy
- Diameter connection is in transport congestion

Severity:
Major

Instance:
<Connection Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterFsmOpStateDegraded

Cause:
This alarm is raised when:

- Connection congestion when the Peer CNDRA Tx sender buffer is at maximum capacity
- The connection's administrative state is enabled and the connection is in congestion. Requests and Answers will continue to be received and processed from the peer over the connection and attempts to send Answers to the peer will still occur. The alarm is raised when one of the following occurs:
  - Connection's Operational Status transitions from available to degraded (connection has become congested or watchdog algorithm has failed)

  - Connection's Operational Status transitions from unavailable to degraded (connection has successfully completed the capabilities exchange and is performing connection proving)
- Connection egress message rate threshold has been crossed
- Diameter connection is in watchdog proving
- Diameter connection is in graceful disconnect
- Diameter peer signaled that the remote is busy
- Diameter connection is in transport congestion

Diagnostic Information:

1. View the Connection Performance measurement report for the +/- 1 hour congestion event.
2. Examine the Log file by using these commands:
   - `# date >> tcp_stat_<hostname>`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# date >> tcp_stat_<hostname>`
3. Examine the output of the command, `netstat -canp --tcp | grep <remote IP:Port for conn>` for few minutes.
4. Examine the corresponding Rx buffer on the connection in question using this command: `netstat -canp --tcp | grep <remote IP:Port for conn>`. The RxBuffer value is configured using **ConnectionCfget**.
5. Examine the overall network statistics for other issues using the command, `netstat -i`.
6. Examine the overall network delay using the command ping.
7. View the software release information.

1. Recovery:

1. View the Connection Performance measurement report for the +/- 1 hour congestion event.
2. Examine the log file by using these commands:
   - `# date >> tcp_stat_<hostname>`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`
   - `# cat /proc/net/tcp >> tcp_stat_<hostname>`
   - `# sleep 1`

- `# cat /proc/net/tcp >> tcp_stat_<hostname>`
- `# sleep 1`
- `# cat /proc/net/tcp >> tcp_stat_<hostname>`
- `# date >> tcp_stat_<hostname>`

3. Examine the output of the command `netstat -canp --tcp | grep <remote IP:Port for conn>` for few minutes.
4. Examine the corresponding Rx buffer on the connection in question using this command:`netstat -canp --tcp | grep <remote IP:Port for conn>`. The RxBuffer value is configured using ConnectionCfget.
5. Examine the overall network statistics for other issues using the command `netstat -i`.
6. Examine the overall network delay using the command `ping`.
7. View the software release information.
8. Identify the most recent Connection Degraded event in the event log for the connection and use the Event's recovery steps to resolve the issue.
9. Have the peer vendor examined their receive buffer usage during the event; if it is 0, this means the received messages were processed quickly and messages were not often stored in the receive buffer. In this case, Egress Transport Congestion was due to the peer not processing the message quickly enough (verify by examining the peer's receive buffer), or there is some delay introduced in the network
10. If the problem persists, it is recommended to contact My Oracle Support.

22103 - SCTP Connection Impaired

Alarm Group:
DIAM

Description:
One or more paths of the SCTP multi-homed connection is down.

Severity:
Minor

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterSCTPConnectionImpairedAlarmNotify

Cause:
A host IP interface for one of the paths in the connection is down. One of following cases can cause this alarm:

- A host IP interface is down
- A host IP interface is unreachable from the peer
- A peer IP interface is down
- A peer IP interface is unreachable from the host
- Network path is down between one host IP and the other peer IP
- Network congestion or large latency in network (resulting loss or late arrival of packets)

Diagnostic Information:

1. Export the Diameter and IPFE configuration information from the active SOAM.
2. Retrieve the software release information.
3. Test each path in the connection to determine which one is causing the connection to be impaired.
4. Capture pcap (tcpdump) trace of packets on the local host (of the specific interface of the MP reporting the issue), or on remote peer or on IPFE (if it is TSA addressed) to see if data traffic or the heartbeat is running on the network

1. Recovery:

1. The alarm clears when the connection is operationally unavailable or all paths are operationally available.

   Potential causes are:

   - A host IP interface is down.
   - A host IP interface is unreachable from the peer.
   - A peer IP interface is down.
   - A peer IP interface is unreachable from the host.
   - Network path is down between one host IP and the other peer IP.
   - Network congestion or large latency in network (resulting loss or late arrival of packets).

2. Identify the most recent SCTP Connection Impaired event in the event log for the connection and use the event's recovery steps to resolve the issue.
3. If the problem persists, it is recommended to contact My Oracle Support.

22104 - SCTP Peer is Operating with a Reduced IP Address Set

Alarm Group:
DIAM

Description:
The SCTP peer advertised less IP addresses than configured for the connection. If two IP addresses have been configured for the Local Node of a certain SCTP connection, but following the SCTP connection establishment the peer node has advertised only one IP address (less than the number of IP addresses configured for the local node), then Alarm 22104 is generated.

Severity:
Minor

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterSCTPPeerReducedIPSetAlarmNotify

Cause:
When the operational status is Available and a connection is established over SCTP transport, the number of IP addresses advertised by the peer in INIT/INIT_ACK is less than the number of paths set by the connection configuration. For instance, the established connection has two IP addresses configured for the Local Node, but the peer node has advertised only one IP address.

Diagnostic Information:
View the networking configuration on the peer node.

1. Recovery:

1. When the operational status is Available and a connection is established over SCTP transport, the number of IP addresses advertised by the peer in INIT/INIT_ACK is less than the number of paths set by the connection configuration. For instance, the established connection has two IP addresses configured for the Local Node, but the peer node has advertised only one IP address.
2. The peer is not able to advertise more than one IP address either due to an error in its configuration or due to being affected by a network interface failure.
3. If the problem persists, it is recommended to contact My Oracle Support.

22105 - Connection Transmit Congestion

Alarm Group:
DIAM

Description:
Alarm is raised when the connection transmit buffer is congested; messages are discarded until condition clears. This error indicates the socket write cannot complete without blocking, which signals the socket buffer is currently full.

Severity:
Major

Instance:
<TransConnName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnectionTxCongestionAlarmNotify

Cause:
The socket write cannot complete without blocking, signaling that the socket buffer is currently full.

Diagnostic Information:
N/A.

1. Recovery:
1. The peer is not able to process the volume of traffic being offered on the connection. Reduce the traffic volume or increase the processing capacity on the peer.
2. If the problem persists, it is recommended to contact My Oracle Support.

22106 - Ingress Message Discarded: DraWorker Ingress MessageRate Control

Alarm Group:
DIAM

Description:
An ingress message is discarded due to connection (or DraWorker) ingress message rate exceeding connection (or DraWorker) maximum ingress MPS.

Severity:
Major

Instance:
<MPHostName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIngressMessageDiscardedAlarmNotify

Cause:
An ingress message is discarded or rejected in the following congestion scenarios:

- Connection maximum message rate exceeded.
- DraWorker maximum message rate exceeded.

Diagnostic Information:

1. From the event history, check the current message rate and the threshold rate for the diameter connection/DAMP node.
2. Check the maximum reserved ingress MPS for the DAMP on the Active Overseer server.
3. Ensure that the ingress MPS is less than the threshold for the diameter connection/DAMP.

1. Recovery:

1. The ingress MPS on the DraWorker is exceeding the MP Maximum ingress MPS. Maybe one or more DraWorkers is unavailable and traffic has been distributed to the remaining DraWorkers.
2. See if one or more peers are generating more traffic than is normally expected.
3. Make sure a sufficient number of DraWorkers is provisioned.
4. If the problem persists, it is recommended to contact My Oracle Support.

22200 - MP CPU Congested

Alarm Group:
ExgStack

Description:
DraWorker CPU utilization threshold has been exceeded. Potential causes are:

- One or more peers are generating more traffic than is normally expected
- Configuration requires more CPUs for message processing than is normally expected
- One or more peers are answering slowly, causing a backlog of pending transactions
- A DraWorker has failed, causing the redistribution of traffic to the remaining DraWorkers

Severity:
Minor, Major, Critical, Warning

Instance
NA

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpCpuCongestedNotify

Cause:
Potential causes are:

- One or more peers are generating more traffic than is normally expected.
- Configuration requires more CPUs for message processing than is normally expected.
- One or more peers are answering slowly, causing a backlog of pending transactions.
- A DraWorker has failed, causing the redistribution of traffic to the remaining DraWorkers.

Diagnostic Information:

1. Observe the ingress traffic rate of each MP.
   a. The misconfiguration of server/client routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transactions per second.
   b. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in congestion, then the traffic load to the server site is exceeding its capacity.
2. Examine the alarm log.
3. Examine the DraWorker status.

1. Recovery:

1. If one or more MPs in a server site has failed, the traffic is distributed between the remaining MPs in the server site. Monitor the **MP** server status.
2. The mis-configuration of DIAMETER peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems. Examine the alarm log.
5. If the problem persists, it is recommended to contact My Oracle Support.

22201 - MpRxAllRate

Alarm Group:
DIAM

Description:
DraWorker ingress message rate threshold crossed.

Severity:
Minor, Major, Critical

Instance:
MpRxAllRate, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpRxAllRateNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If the problem persists, it is recommended to contact My Oracle Support.

22202 - MpDiamMsgPoolCongested

Alarm Group:
DIAM

Description:
DraWorker Diameter message pool utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
MpDiamMsgPool, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpDiamMsgPoolCongestedNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PDU buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted.

5. If the problem persists, it is recommended to contact My Oracle Support.

22203 - PTR Buffer Pool Utilization

Alarm Group:
DIAM

Description:
The MP's PTR buffer pool is approaching its maximum capacity. If this problem persists and the pool reaches 100% utilization all new ingress messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPtrBufferPoolUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. A software defect may exist resulting in PTR buffers not being deallocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted.
5. If the problem persists, it is recommended to contact My Oracle Support.

22204 - Request Message Queue Utilization

Alarm Group:
DIAM

Description:
The MP's Request Message Queue Utilization is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress Request messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRequestMessageQueueUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the Request Task may be experiencing a problem preventing it from processing messages from its Request Message Queue.
5. If the problem persists, it is recommended to contact My Oracle Support.

22205 - Answer Message Queue Utilization

Alarm Group:
DIAM

Description:
The MP's Answer Message Queue Utilization is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization all new ingress Answer messages will be discarded. This alarm should not normally occur when no other congestion alarms are asserted.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterAnswerMessageQueueUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. If no additional congestion alarms are asserted, the Answer Task may be experiencing a problem preventing it from processing messages from its Answer Message Queue.
5. If the problem persists, it is recommended to contact My Oracle Support.

22206 - Reroute Queue Utilization

Alarm Group:
DIAM

Description:
The MP's Reroute Queue is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization any transactions requiring rerouting will be rejected. This alarm should not normally occur when no other congestion alarms are asserted.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRerouteQueueUtilNotify

1. Recovery:

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer time-outs.
2. If no additional congestion alarms are asserted, the Reroute Task may be experiencing a problem preventing it from processing messages from its Reroute Queue.
3. If the problem persists, it is recommended to contact My Oracle Support.

22207 - DclTxTaskQueueCongested

Alarm Group:
DIAM

Description:
DCL egress task message queue utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<DraWorker Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDclTxTaskQueueCongested

1. Recovery:

1. The alarm will clear when the DCL egress task message queue utilization falls below the clear threshold. The alarm may be caused by one or more peers being routed more traffic than is nominally expected.
2. If the problem persists, it is recommended to contact My Oracle Support.

22208 - DclTxConnQueueCongested

Alarm Group:
DIAM

Description:
DCL egress connection message queue utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<ConnectionName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDclTxConnQueueCongested

1. Recovery:

1. The alarm will clear when the DCL egress connection message queue utilization falls below the clear threshold. The alarm may be caused by peers being routed more traffic than nominally expected.
2. It is recommended to contact My Oracle Support for further assistance.

22209 - Message Copy Disabled

Alarm Group:
DIAM

Description:
Diameter Message Copy is disabled.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMessageCopyDisabledNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed between the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. The Diameter Process may be experiencing problems.
5. If the problem persists, contact My Oracle Support.

22214 - Message Copy Queue Utilization

Alarm Group:
DIAM

Description:
The DraWorker's Message Copy queue utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMsgCopyQueueUtilNotify

1. Recovery:

1. Reduce traffic to the MP.
2. Verify that no network issues exist between the DraWorker and the intended DAS peer(s).
3. Verify that the intended DAS peer has sufficient capacity to process the traffic load being routed to it.
4. If the problem persists, it is recommended to contact My Oracle Support.

22221 - Routing MPS Rate

Alarm Group:
DIAM

Description:
Message processing rate for this MP is approaching or exceeding its engineered traffic handling capacity. The routing mps rate (MPS/second) is approaching or exceeding its engineered traffic handling capacity for the MP.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRoutingMpsRateNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site.
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP.

   Each MP in the server site should be receiving approximately the same ingress transaction per second.

3. There may be an insufficient number of MPs configured to handle the network traffic load.

   If all MPs are in a congestion state then the ingress message rate to the MP is exceeding its capacity to process the messages.

4. If the problem persists, it is recommended to contact My Oracle Support.

22222 - Long Timeout PTR Buffer Pool Utilization

Alarm Group:
DIAM

Description:
The MP's Long Timeout PTR buffer pool is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterLongTimeoutPtrBufferPoolUtilNotify

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site.
2. The misconfiguration of Pending Answer Timer assignment may result in excessive traffic being assigned to the Long Timeout PTR buffer Pool.
3. The misconfiguration of Diameter peers may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transaction per second
4. There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
5. A software defect may exist resulting in Long Timeout PTR buffers not being de-allocated to the pool. This alarm should not normally occur when no other congestion alarms are asserted. Examine the alarm log.
6. If the problem persists, it is recommended to contact My Oracle Support.

22223 - DraWorker Memory Utilization Threshold Crossed

Alarm Group:
DIAM

Description:
DraWorker memory utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
System.RAM_UtilPct, Peer CNDRA

HA Score:
Normal

Auto Clear Seconds:
0 (zero, no auto clear)

OID:
eagleXgDiameterMpMemCongestedNotify

Cause:
Following are the potential causes:

- One or more peers are generating more traffic than expected.
- Configuration requires more Physical Memory for message processing than expected.
- One or more peers are answering slowly, causing a backlog of pending transactions.
- A DraWorker failed, causing the redistribution of traffic to the remaining DraWorkers.

Diagnostic Information:
To diagnose the cause:

1. Monitor the ingress traffic rate of each MP.
    - The mis-configuration of server/client routing may result in too much traffic being distributed to the MP. Each MP in the server site should be receiving approximately the same ingress transactions per second.
    - There may be an insufficient number of MPs configured to handle the network traffic load. If all MPs are in congestion, then the traffic load to the server site is exceeding its capacity.
2. Examine the alarm log.
3. Examine the DraWorker status.

1. Recovery:

1. Analyze and correct routing so the traffic load is balanced between MPs.
2. If all MPs are approaching or exceeding their engineered traffic handling capacity, add more MPs to the system and configure connections and routes to distribute traffic to new DraWorkers.
3. If the problem persists, it is recommended to contact My Oracle Support.

22224 - Average Hold Time Limit Exceeded

Alarm Group:
DIAM

Description:
The average transaction hold time has exceeded its configured limits.
This alarm is generated when KPI #10098 (TmAvgRspTime) exceeds Peer CNDRA-wide engineering attributes associated with average hold time, defined in the DraWorker profile assigned to the DraWorker server. KPI #10098 is defined as the average time (in milliseconds) from when the routing layer (DRL) receives a request message from a downstream peer to the time that an answer response is sent to that downstream peer. The source measurement of KPI #10098 is the TmResponseTimeDownstreamMp (10093) measurement.
This alarm indicates the average response time (TmAvgRspTime) for messages forwarded by the Relay Agent is larger than what is defined for a deployment as per DraWorker profile assignment. One of these problems could exist:

- The IP network may be experiencing problems that are adding propagation delays to the forwarded request message and the answer response.
  - Verify the IP network connectivity exists between the MP server and the adjacent nodes.
  - View the event history logs for additional events or alarms from this MP server.
- One or more upstream nodes may be experiencing traffic overload.
- One or more MPs is experiencing traffic overload.
  - View the KPI Routing Recv Msgs/Sec.
  - View the CPU utilization of MPs.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterAvgHoldTimeLimitExceededNotify

Cause:
Alarm 22224 is generated when KPI #10098 (TmAvgRspTime) exceeds Peer CNDRA-wide engineering attributes associated with average hold time, defined in the DraWorker profile assigned to the DraWorker server. KPI #10098 is defined as the average time (in milliseconds) from when the routing layer (DRL) receives a request message from a downstream peer to the time that an answer response

is sent to that downstream peer. The source measurement of KPI #10098 is the TmResponseTimeDownstreamMp (10093) measurement.
The alarm thresholds are configurable for:

- Average hold time minor alarm onset threshold
- Average hold time minor alarm abatement threshold
- Average hold time major alarm onset threshold
- Average hold time major alarm abatement threshold
- Average hold time critical alarm onset threshold
- Average hold time critical alarm abatement threshold

The severity of the alarm (Minor, Major, or Critical) is according to onset threshold/ abatement threshold of each severity level. When the average hold time initially exceeds the average hold time for an alarm onset threshold, a minor, major, or critical alarm is triggered. When the average hold time subsequently exceeds a higher onset threshold, or drops below an abatement threshold, but is still above the minor alarm abatement threshold, the alarm severity changes based on the highest onset threshold crossed by the current average hold time.

Diagnostic Information:
If Alarm #22224 is raised, then it indicates the average response time (TmAvgRspTime) for messages forwarded by the Relay Agent is larger than the defined for a deployment as per DraWorker profile assignment. One of the following problems could exist:

- The IP network may be experiencing problems that are adding propagation delays to the forwarded request message and the answer response.
  - Verify the IP network connectivity exists between the MP server and the adjacent nodes.
  - View the event history logs for additional events or alarms from this MP server.
- The IP network may be experiencing problems that are adding propagation delays to the forwarded request message and the answer response.
- One or more upstream nodes may be experiencing traffic overload.
- One or more MPs is experiencing traffic overload.
  - View the KPI Routing Recv Msgs/Sec.
  - View the CPU utilization of MPs.

1. Recovery:

1. The average transaction hold time is exceeding its configured limits, resulting in an abnormally large number of outstanding transactions that may be leading to excessive use of resources like memory.
   - Reduce the average hold time by examining the configured Pending Answer Timer values and reducing any values that are unnecessarily large or small.
   - Identify the causes for the large average delay between the Peer CNDRA sending requests to the upstream peers and receiving answers for the requests.
   - Confirm the peer node(s) or Peer CNDRA is in overload by viewing KPI/ Measurements/CPU usage and take corrective action.

- Identify the main contributor to increased value of (T2-T1) such as a time difference between the routing layer (DRL) receiving the request to the DRL sending the answer to downstream peer.

2. The alarm thresholds are configurable for:
   - Average hold time minor alarm onset threshold
   - Average hold time minor alarm abatement threshold
   - Average hold time major alarm onset threshold
   - Average hold time major alarm abatement threshold
   - Average hold time critical alarm onset threshold
   - Average hold time critical alarm abatement threshold

   The severity of the alarm (Minor, Major, or Critical) is according to the onset threshold/abatement threshold of each severity level. When the average hold time initially exceeds the average hold time for an alarm onset threshold, a minor, major, or critical alarm is triggered. When the average hold time subsequently exceeds a higher onset threshold, or drops below an abatement threshold, but is still above the minor alarm abatement threshold, the alarm severity changes based on the highest onset threshold crossed by the current average hold time.
3. If the problem persists, it is recommended to contact My Oracle Support.

22225 - Average Message Size Limit Exceeded

Alarm Group:
DIAM

Description:
The size of the average message processed by Peer CNDRA has exceeded its configured limits.
The alarm is generated when the measurement RxAvgMsgSize reaches the Peer CNDRA-wide engineering attributes, defined in the DaMpProfileParameters corresponding to the MP profile being used. RxAvgMsgSize is defined as the size of the average message processed by Peer CNDRA.
This alarm indicates Peer CNDRA has encountered a message it can accept for processing, but might not continue processing if the message size increases more than the maximum supported message size. This increase can be due to standard diameter processing (for example, Route Record additions to requests) or due to custom processing (for example, Mediation modifying AVPs).

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterAvgMsgSizeLimitExceededNotify

Cause:
Alarm 22225 raises when the measurement RxAvgMsgSize reaches the Peer CNDRA-wide engineering attributes, defined in the DaMpProfileParameters corresponding to the MP profile being used.
RxAvgMsgSize is defined as the size of the average message processed by Peer CNDRA.

- Average message size minor alarm onset threshold
- Average message size minor alarm abatement threshold
- Average message size major alarm onset threshold
- Average message size major alarm abatement threshold
- Average message size critical alarm onset threshold
- Average message size critical alarm abatement threshold

The severity of alarm (Minor, Major, or Critical) is according to onset/abatement threshold of each severity level. When the average message size reaches the value of the respective alarm onset/abatement threshold, within 3 seconds the alarm is raised with severity Minor, Major, or Critical, based on the value reached by the average message size.

Diagnostic Information:
This event indicates that Peer CNDRA has encountered a message that it can accept for processing, but might not continue processing if the message size increases more than the maximum supported message size. This increase can be due to standard diameter processing (for example, RouteRecord additions to requests) or due to custom processing (for example, Mediation modifying AVPs).

1. Recovery:

1. Examine the traffic coming from connected peers to see if any of them are sending abnormally large messages, and look for any special processing rules being applied by Peer CNDRA to that message.
2. The alarm thresholds are configurable for:
   - Average hold time minor alarm onset threshold
   - Average hold time minor alarm abatement threshold
   - Average hold time major alarm onset threshold
   - Average hold time major alarm abatement threshold
   - Average hold time critical alarm onset threshold
   - Average hold time critical alarm abatement threshold

   The severity of the alarm (Minor, Major, or Critical) is according to the onset threshold/abatement threshold of each severity level. When the average hold time initially exceeds the average hold time for an alarm onset threshold, a minor, major, or critical alarm is triggered. When the average hold time subsequently exceeds a higher onset threshold, or drops below an abatement threshold, but is still above the minor alarm abatement threshold, the alarm severity changes based on the highest onset threshold crossed by the current average hold time.
3. If the problem persists, it is recommended to contact My Oracle Support.

22328 - Connection is processing a higher than normal ingress messaging rate

Alarm Group:
DIAM

Description:
The diameter connection specified in the alarm instance is processing a higher than normal ingress messaging rate.

Severity:

- Minor (if all of the following are true):
  - The average ingress MPS rate the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection minor alarm threshold.
  - The average ingress MPS rate the connection is processing has not yet reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.
- Major (if the following are true):
  - The average ingress MPS rate the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

Instance:
The name of the diameter connection as defined by the TransportConnection table

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIngressMpsRateNotify

Cause:
Alarm # 22328 raises the severity,

Minor (if all of the following are true):

- The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection minor alarm threshold.
- The average ingress MPS rate that the connection is processing has not yet reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

Major (if all of the following are true):

- The average ingress MPS rate that the connection is processing has reached the percentage of the connection's maximum ingress MPS rate configured for the connection major alarm threshold.

Diagnostic Information:
To get further information regarding this issue:

1. Examine the alarm log on Active Overseer Server.
2. Get the Connection ID **IcRate[Connection_Id]** from Alarm Details and the corresponding Connection Name from **TransportConnectionTable** on active Overseer server.
3. Investigate the connection's remote Diameter peer (the source of the ingress messaging) to determine why they are sending the abnormally high traffic rate.

1. Recovery:

1. The Diameter connection specified in the Alarm Instance field is processing a higher than expected average ingress Diameter message rate. The alarm thresholds for minor and major alarms are configured in the Capacity Configuration Set used by the Diameter connection.
2. The message rate used for this alarm is an exponentially smoothed 30 second average. This smoothing limits false alarms due to short duration spikes in the ingress message rate.
3. If the alarm severity is minor, the alarm means the average ingress message rate has exceeded the minor alarm threshold percentage of the maximum ingress MPS configured for the connection.
4. If the alarm severity is major, the alarm means the average ingress message rate has exceeded the major alarm threshold percentage of the maximum ingress MPS configured for the connection.
5. This alarm is cleared when the average ingress message rate falls 5% below the minor alarm threshold, or the connection becomes disabled or disconnected. This alarm is downgraded from major to minor if the average ingress message rate falls 5% below the major alarm threshold.
6. If the average ingress message rate is determined to be unusually high, investigate the connection's remote Diameter peer (the source of the ingress messaging) to determine why they are sending the abnormally high traffic rate; otherwise, consider increasing either the connection's maximum ingress MPS rate or the connection's alarm thresholds.
7. If the problem persists, it is recommended to contact My Oracle Support.

22349 - IPFE Connection Alarm Aggregation Threshold

Alarm Group:
DIAM

Description:
This alarm occurs when there are a ‘Critical’ number of IPFE connection alarms for the network element.
The Alarm Thresholds are configurable using the Alarm Threshold Options tab on **Diameter**, and then **Configuration**, and then **System Options**.

The IPFE connection may not be established for a variety of reasons. The operational status of this connection is displayed on the GUI as unavailable and Alarm 22101 Connection Unavailable is raised.
When the number of unavailable IPFE connections exceeds the defined threshold, IPFE Connection Failure Major/Critical Aggregation Alarm Threshold (default is 100/200), alarm 22349 is raised by the DSR.

Severity:
Major, Critical

> **Note:**
>
> The Critical threshold may be disabled by setting the Critical Threshold to zero using the Alarm Threshold Options tab on **Diameter**, and then **Configuration**, and then **System Options**.

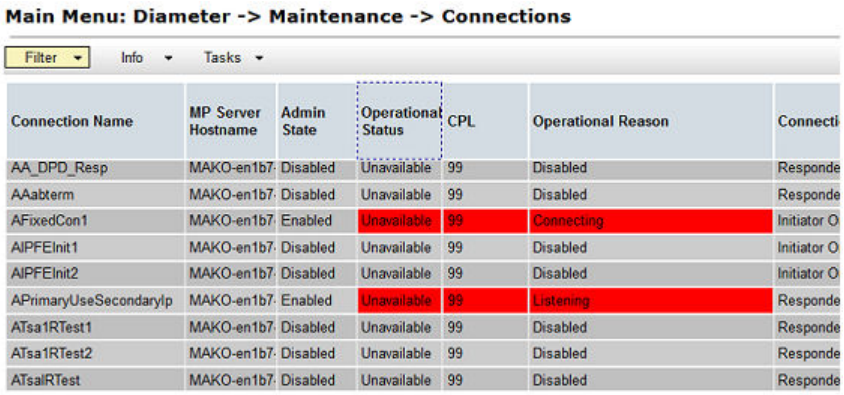
Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIPFEConnUnavailableThresholdReachedNotify

Cause:
The IPFE connection may not be established for a variety of reasons. The operational status of this connection is displayed on the GUI as unavailable and Alarm 22101, Connection Unavailable is raised.



When the number of unavailable IPFE connections exceeds the defined threshold, IPFE Connection Failure Major/Critical Aggregation Alarm Threshold (default is 100/200), alarm 22349 is raised by the DSR.

Diagnostic Information:
Perform the following:

- Use Wireshark to capture the diameter traffic on all MPs under the concerned TSA list and the primary IPFE. Save the PCAP traffic capture generated by Wireshark.
- Verify the connection configurations (IP addresses, ports, peer node, protocol) are correct.
- Verify peer-connection configurations (protocol, remote/local IP address, remote/local port) matches local connection configurations.
- Verify the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.

1. Recovery:

1. Navigate to **Diameter**, and then **Maintenance**, and then **Connection** to monitor IPFE Connection status.
2. Confirm peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm the connection’s transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.
4. Verify the peers in the Route List are not under maintenance.
5. Use Wireshark to analyze all the captured PCAP data to find where the message exchange is broken or failed. Wireshark should be the main tool used to diagnose the unavailable connection.
6. Based on the PCAP file, correct the configuration if the issue is on the DSR side. The Alarm will be cleared automatically when the numbers of unavailable IPFE connections are under the IPFE Connection Failure Critical/Major Aggregation Alarm Threshold.
7. If the issue is on the DSR side or you are not sure, it is recommended to contact My Oracle Support for assistance.

22350 - Fixed Connection Alarm Aggregation Threshold

Alarm Group:
DIAM

Description:
This alarm occurs when there are a critical number of fixed connection alarms for the DraWorker.

Severity:
Major, Critical

> **Note:**
>
> The Critical threshold may be disabled by setting the Critical Threshold to zero.

Instance:
<DraWorker-Hostname>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnUnavailableThresholdReachedNotify

Cause:
The alarm #22350 raises when there are a critical number of fixed connection alarms for the DraWorker.

Diagnostic Information:
To get further information regarding this issue:

1. Find all the connections with a problem for the specific MP.
2. For each connection with a problem, verify:
   a. The remote host is reachable from the local MP by using ssh to the MP and pinging the remote server IP (if using IP address) or server FQDN (if using FQDN)
   b. DNS availability should be tested by pinging the DNS server IP
   c. FQDN resolving should be tested by using nslookup to check the FQDN resolving on the MP
3. If the above tests reveal the remote host is not reachable, then verify that there is no network problem on the remote server.
4. If the remote server is reachable, then verify the processes are running correctly.
   a. Verify the local Peer CNDRA process is running by checking the `ps -ef` output
   b. Verify the local node is listening on the correct port by using `netstat -na` and checking the correct transport type, tcp/sctp port is listening
   c. Use wireshark or tcpdump to capture traffic messages, and verify the connection is established (confirm the handshake process is occurring for SCTP or TCP)
5. If the port is not listening, or the handshake procedure is not occurring, then the process or server may be in trouble.
6. If the connection/association is established, then ensure that the Diameter handshake is happening and correct, by checking the Diameter CEX message exchange, for information like server FQDN, IP address, or applications supported; mismatching information causes the connection to abort.
7. If Diameter handshake is good, then observe the health of the Diameter connection by verifying the DWR messages are answered correctly.

1. Recovery:

1. Check Fixed Connection status.
2. Confirm the peer connection configuration (protocol, remote/local IP address, remote/local port) matches the local connection configuration.
3. Confirm the connection's transport protocol and/or port are not being blocked by a network firewall or other ACL in the network path.

4. Verify the peers in the Route List are not under maintenance.
5. Modify the value of **Alarm Threshold Options** if it is set too low.
6. It is recommended to contact My Oracle Support for assistance.

22900 - DPI DB Table Monitoring Overrun

Event Type:
DIAM

Description:
The COMCOL update sync log used by DB Table monitoring to synchronize Diameter Connection Status among all DraWorker RT-DBs has overrun. The DraWorker's Diameter Connection Status sharing table is automatically audited and re-synced to correct any inconsistencies.

Severity:
Info

Instance:
<DbTblName>

> **Note:**
>
> <DbTblName> refers to the name of the Diameter Connection Status Sharing Table the Diameter Connection status inconsistency that was detected.

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDpiTblMonCbOnLogOverrunNotify

1. Recovery:

- It is recommended to contact My Oracle Support if this alarm is constantly being asserted and cleared.

22901 - DPI DB Table Monitoring Error

Event Type:
DIAM

Description:
An unexpected error occurred during DB Table Monitoring.

Severity:
Info

Instance:
DpiTblMonThreadName

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDpiSldbMonAbnormalErrorNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

22950 - Connection Status Inconsistency Exists

Alarm Group:
DIAM

Description:
Diameter Connection status inconsistencies exist among the DraWorkers in the Peer CNDRA signaling NE.

Severity:
Critical

Instance:
<DbTblName> Name of the Diameter Connection Status Sharing Table where the Diameter Connection status inconsistency was detected.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnStatusInconsistencyExistsNotify

Cause:
The data inconsistency might have caused due to the following reasons:

- Network issue, the change log is not distributed to the destination MP.
- Process error (update is disturbed) in executing change on the destination MP.

Diagnostic Information:
No specific diagnostic information is required if alarm clears in the next audit/sync. Analyze the error log if the problem persists.

1. Recovery:

- No action necessary.

> **Note:**
>
> DraWorker's SLDB tables are automatically audited and re-synchronized to correct inconsistencies after a log overrun has occurred. The Automatic Data Integrity Check, which was introduced in cm6.2, periodically scans almost the entire local IDB for integrity. The initial default period is 30 minutes.

22960 - DA-MP Profile Not Assigned

Alarm Group:
DIAM

Description:
This alarm is generated when a DA-MP is brought into service and a DA-MP configuration profile has not been assigned to the DA-MP during DSR installation/ upgrade procedures.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDaMpProfileNotAssignedNotify

Cause:
Alarm #22960 raises when a DA-MP is brought into service and a DA-MP configuration profile has not been assigned to the DA-MP during DSR installation/ upgrade procedures.

Diagnostic Information:
Examine the error log in **Main Menu > Alarms & Events**.

1. Recovery:
1. From the DSR OAM GUI, navigate to **Diameter Common**, and then **MPs**, and then **Profile Assignments** to assign a DA-MP profile to the DA-MP.
2. If the problem persists, it is recommended to contact My Oracle Support.

22961 - Insufficient Memory for Feature Set

Alarm Group:
DIAM

Description:
The available memory (in kilobytes) for feature set is less than the required memory (in kilobytes). This alarm is raised when a DraWorker is brought into service and a DraWorker configured DiamaterMaxMessageSize in DpiOption table value is greater than 16KB, but the available memory on DraWorker is less than 48GB.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterInsufficientAvailMemNotify

Cause:
Alarm #22961 raises when a DraWorker is brought into service and a DraWorker configured DiamaterMaxMessageSize in DpiOption table value is greater than 16KB but the available memory on DraWorker is less than 48GB.

Diagnostic Information:
N/A.

1. Recovery:

1. Make additional memory available on the DraWorker for the configured DiameterMaxMessageSize.
2. If the problem persists, it is recommended to contact My Oracle Support.

25607 - DSR Signaling Firewall is administratively Disabled

Alarm Group
DIAM

Description
DSR Signaling Firewall is administratively Disabled

Severity
Minor

Instance
<System OAM name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterFwDisabledNotify

1. Recovery

1. Navigate to the Signaling Firewall page (**Diameter**, and then **Maintenance**, and then **Signaling Firewall**). Click the **Enable** button.
2. If the problem persists, it is recommended to contact My Oracle Support.

25608 - Abnormal DA-MP Firewall

Alarm Group
DIAM

Description
DSR Signaling Firewall Operational status is degraded.

Severity
Minor

Instance
<DA-MP name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterFwDegradedNotify

1. Recovery

1. Analyze event 25609 - Firewall Configuration Error encountered to identify the error(s) and the DA-MP which reported the error(s).
2. Analyze any platform alarms on the identified DA-MP. Follow the procedures to clear the platform alarms on the identified DA-MP
3. Disable the Signaling Firewall from the Signaling Firewall page (**Diameter**, and then **Maintenance**, and then **Signaling Firewall**).
4. If the alarm persists, restart the application on the identified DA-MP from the **Status & Manage** screen on the active Network OAM GUI.
5. If the problem is still unresolved, it is recommended to contact My Oracle Support for assistance.

25609 - Firewall Configuration Error encountered

Event Type
DIAM

Description
Firewall Configuration Error encountered.

Severity
Info

Instance
<DA-MP name>

HA Score
Normal

Throttle Seconds
N/A

OID
eagleXgDiameterFwDisabledNotify

1. Recovery

- This event is unexpected. It is recommended to contact My Oracle Support for analysis and resolution.

25610 - DSR Signaling Firewall configuration inconsistency detected

Alarm Group
DIAM

Description
DSR Signaling Firewall configuration inconsistency detected

Severity
Minor

Instance
<DA-MP name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterFwDegradedNotify

1. Recovery

1. One possible cause could be manual changes in the "01dsr" domain of Linux firewall configuration on the DA-MP server. If so, the manual configuration should be rolled back.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25611 - ETG - Invalid DRMP Attributes

Alarm Group
DIAM

Description
DRMP attributes of ETG not in synch with remote ETGs associated with same ETL.

Severity
Minor

Instance
<ETG name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterEtgInvalidDRMPAttrbsNotify

1. Recovery

- If the problem persists, it is recommended to contact My Oracle Support for assistance.

25612 - Peer CNDRA ping failed

Alarm Group
DIAM

Description
Connection was rejected due to the DraWorker exceeding its connection or ingress MPS capacity

Severity
Major

Instance
pingAllLivePeers

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterPingAllLivePeerErrorNotify

1. Recovery
1. Check `/var/log/messages` and `/var/log/cron` for more information.
2. Run `pingAllLivePeers -v` and `pingAllLivePeers -h` as root on the command line.
3. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25613 – Peer Node Alarm Group Threshold

Event Type:
DIAM

Description:
Peer Node Alarm Group Threshold Reached. This alarm occurs when there are a number of minor, major, or critical Peer Node alarms for a single Peer Node Alarm Group.

Severity:
Minor, Major, and Critical

Instance:
<PeerNodeAlarmGroupName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterPeerNodeAlarmGroupThresholdReachedNotify

1. Check status of Peer nodes.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Verify the peer is not under maintenance.
4. It is recommended to contact My Oracle Support if further assistance is needed.

25614 - Connection Alarm Group Threshold

Event Type:
DIAM

Description:
Connection Alarm Group Threshold Reached. This alarm occurs when there are a number of minor, major, or critical Connection alarms for a single Connection Alarm Group.

Severity:
Minor, Major, and Critical

Instance:
<ConnectionAlarmGroupName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterConnectionAlarmGroupThresholdReachedNotify

1. Check Connections status.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Verify the connection is not under maintenance.
4. It is recommended to contact My Oracle Support if further assistance is needed.

25805 - Invalid Shared TTG Reference

Alarm Group
DIAM

Description
Invalid Shared TTG Reference

Severity
Minor

Instance
<Route List Name>&<Route Group Name>&<TTG SG Name>&<TTG Name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterDoicInvalidSharedTtgRefNotify

1. Recovery

1. For the Route List named in the alarm instance, edit its configuration and delete the association to the non-existent Shared TTG. Then,
2. If desired, re-create the Shared TTG at its host site, and re-add the association to the Route List/Route Group.

> **Note:**
>
> Because, internally, the association of a TTG to the RL/RG is based on an internal ID, (not the TTG name), it is not valid to leave the original association in the Route List configuration and simply create a new Shared TTG with original name. This will not work, as the internal ID for the original TTG will not be the same as the ID for the new TTG (even though the TTG name is the same).

25806 - Invalid Internal Overseer Server Group Designation

Alarm Group
DIAM

Description
Invalid Internal Overseer Server Group Designation

Severity
Minor

Instance
<Route List Name>&<Route Group Name>&<TTG SG Name>&<TTG Name>

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterDoicInvalidInternalSoamSgDesignationNotify

1. Recovery

- For the Route List named in the alarm instance, edit its configuration and delete the association to the Shared TTG. This will clear the alarm. The association can simply be re-added to restore integrity to the configuration.

Range Based Address Resolution (RBAR) Alarms and Events (22400-22424)

22400 - Message Decoding Failure

Event Type:
RBAR

Description:
A message received was rejected because of a decoding failure.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarMsgRejectedDecodingFailureNotify

1. Recovery:

- While parsing the message, the message content was inconsistent with the Message Length in the message header. These protocol violations can be caused by the originator of the message (identified by the Origin-Host AVP in the message) or the peer who forwarded the message to this node.

22401 - Unknown Application ID

Event Type:
RBAR

Description:
A message could not be routed because the Diameter Application ID is not supported.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarUnknownApplIdNotify

1. Recovery:

1. The Peer CNDRA **Relay Agent** forwarded a Request message to the address resolution application which contained an unrecognized Diameter Application ID in the header. Either a Peer CNDRA **Relay Agent** application routing rule is mis-provisioned or the Application ID is not provisioned in the RBAR routing configuration.
2. Check the currently provisioned Diameter Application IDs.
3. Check the currently provisioned Application Routing Rules.

22402 - Unknown Command Code

Event Type:
RBAR

Description:
A message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarUnknownCmdCodeNotify

1. Recovery:

1. The order pair (Application ID, Command Code) is not provisioned in the Address Resolutions routing configuration.
2. Check the currently provisioned Application IDs and Command Codes.

22403 - No Routing Entity Address AVPs

Event Type:
RBAR

Description:
A message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.

Severity:
Info

Instance:
<AddressResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarNoRoutingEntityAddrAvpNotify

1. Recovery:

1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. Check the currently provisioned Application IDs and Command Codes.

22404 - No valid Routing Entity Addresses found

Event Type:
RBAR

Description:
A message could not be routed because none of the address AVPs contained a valid address and the Routing Exception was configured to send an Answer response.

Severity:
Info

Instance:
<AddressResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarNoValidRoutingEntityAddrFoundNotify

1. Recovery:
1. This may be a normal event or an event associated with misprovisioned address resolution configuration. If this event is considered abnormal, validate which AVPs are configured for routing with the Application ID and Command Code.
2. Check the currently provisioned Application IDs and Command Codes.

22405 - Valid address received didn't match a provisioned address or address range

Event Type:
RBAR

Description:
A message could not be routed because a valid address was found that did not match an individual address or address range associated with the Application ID, Command Code, and Routing Entity Type, and the Routing Exception was configured to send an Answer response.

Severity:
Info

Instance:
<AddressResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarAddrMismatchWithProvisionedAddressNotify

1. Recovery:

1. An individual address or address range associated with the Application ID, Command Code and Routing Entity Type may be missing from the RBAR configuration. Validate which address and address range tables are associated with the Application ID, Command Code and Routing Entity Type.
2. View the currently provisioned Application IDs, Command Codes, and Routing Entity Types by selecting **RBAR**, and then **Configuration**, and then **Address Resolutions**.

22406 - Routing attempt failed due to internal resource exhaustion

Event Type:
RBAR

Description:
A message could not be routed because the internal "Request Message Queue" to the Peer CNDRA Relay Agent was full. This should not occur unless the MP is experiencing local congestion as indicated by Alarm-ID 22200 - MP CPU Congested.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarRoutingAttemptFailureInternalResExhNotify

1. Recovery:

- If this problem occurs, it is recommended to contact My Oracle Support.

22407 - Routing attempt failed due to internal database inconsistency failure

Event Type:
RBAR

Description:
A message could not be routed because an internal address resolution run-time database inconsistency was encountered.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterRbarRoutingFailureInternalDbInconsistencyNotify

1. Recovery:

- If this problem occurs, it is recommended to contact My Oracle Support.

22411 - Address Range Lookup for Local Identifier skipped

Alarm Group:
RBAR

Description:
Address Range Lookup could not be performed for the Local Identifier component of the Routing Entity Type External Identifier. Address Resolution used the Destination found using Domain Identifier.

Severity:
Info

Instance:
xxx

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
xxx

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

Generic Application Alarms and Events (22500-22599)

> **Note:**
>
> These alarms are generic across the various Peer CNDRA applications with some details varying depending on the application generating the alarm.

22500 - Peer CNDRA Application Unavailable

Alarm Group:
APPL

Description:
Peer CNDRA application is unable to process any messages because it is unavailable.

Severity:
Critical

Instance:
<Peer CNDRA Application Name>

> **Note:**
>
> The value for Peer CNDRA Application Name varies depending on the Peer CNDRA application generating the alarm such as RBAR. Use the name that corresponds to the specific Peer CNDRA application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCndraApplicationUnavailableNotify

Cause:
The alarm #22500 is raises:

- When the Peer CNDRA application completes initialization and determines its operational status is unavailable after changing its admin state from disabled to enabled.
- When the Peer CNDRA application is in enabled state and the following Peer CNDRA application operational status changes occur:
  - Available → Unavailable

  - Degraded → Unavailable

This alarm is clears:

- When Peer CNDRA application is in enabled state and the following Peer CNDRA application operational status changes occur:
  - Unavailable → Available
  - Unavailable → Degraded
- If the Diameter process is stopped.
- If the Peer CNDRA application admin state change from Enabled > Disabled.

Diagnostic Information:

- A Peer CNDRA application operation status becomes unavailable when either the Admin State is set to Disable with the Forced Shutdown option, or the Admin State is set to Disable with the Graceful Shutdown option and the Graceful Shutdown timer expires.
- A Peer CNDRA application can also become unavailable when it reaches Congestion Level 3 if enabled.

> **Note:**
>
> This alarm is NOT raised when the Peer CNDRA application is shutting down gracefully or application is in Disabled state. Only the Peer CNDRA Application operational status is changed to unavailable.

1. Recovery:

1. Display and monitor the Peer CNDRA application status. Verify the Admin State is set as expected.
2. A Peer CNDRA application operation status becomes unavailable when either the Admin State is set to disable with the Forced Shutdown option, or the Admin State is set to disable with the Graceful Shutdown option and the Graceful Shutdown timer expires.
3. If the problem persists, it is recommended to contact My Oracle Support.

22501 - Peer CNDRA Application Degraded

Alarm Group:
APPL

Description:
Unable to forward requests to the Peer CNDRA application because it is degraded.

Severity:
Major

Instance:
<Peer CNDRA Application Name>

> **Note:**
>
> The value for Peer CNDRA Application Name varies depending on the Peer CNDRA application generating the alarm such as RBAR. Use the name that corresponds to the specific Peer CNDRA application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCndraApplicationDegradedNotify

Cause:
The alarm #22501 raises when the Peer CNDRA application is in enabled state and the following Peer CNDRA Application Operational Status changes occur:

- Available → Degraded
- Unavailable → Degraded

This alarm is cleared when the Peer CNDRA application is in enabled state and following Peer CNDRA Application Operational Status changes occur:

- Degraded → Available
- Degraded → Unavailable

Diagnostic Information:

- A Peer CNDRA application becomes degraded when the Peer CNDRA application becomes congested if enabled. This alarm is NOT raised when the Peer CNDRA application is shutting down gracefully or application is in the disabled state.
- Verify the admin state is set as expected. Check the Event History logs for additional DIAM events or alarms from this MP server.

1. Recovery:

1. Check the Peer CNDRA application status. Verify the Admin State is set as expected.
2. A Peer CNDRA application becomes degraded when the Peer CNDRA application becomes congested, if enabled.

> **Note:**
>
> This alarm is NOT raised when the Peer CNDRA application is shutting down gracefully or application is in the disabled state. Only the Peer CNDRA application operational status is changed to unavailable.

3. Check the Event History logs for additional DIAM events or alarms for this **MP** server.
4. If the problem persists, it is recommended to contact My Oracle Support.

22502 - Peer CNDRA Application Request Message Queue Utilization

Alarm Group:
APPL

Description:
The Peer CNDRA Application Request Message Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
<Metric ID>, <Peer CNDRA Application Name>

> **Note:**
>
> The value for Metric ID for this alarm varies (such as RxRbarRequestMsgQueue) depending on which Peer CNDRA application generates the alarm (such as RBAR). Use the ID that corresponds to the specific Peer CNDRA application in use.

> **Note:**
>
> The value for Peer CNDRA Application Name will vary depending on the Peer CNDRA application generating the alarm (such as RBAR). Use the name that corresponds to the specific Peer CNDRA application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCndraApplicationRequestQueueUtilNotify

Cause:
Alarm #22502 is raises:

- When Peer CNDRA Application Request Message Queue Utilization is approaching its maximum capacity.
- If this problem persists and the queue reaches 100% utilization all new ingress Request messages will be discarded.

Diagnostic Information:
To get further information regarding this issue:

1. Examine the alarm log on the active Overseer server.

2. This alarm should not normally occur when no other congestion alarms are asserted.

1. Recovery:

1. Display and monitor the Peer CNDRA application status. Verify the Admin State is set as expected.

   The Peer CNDRA application's Request Message Queue Utilization is approaching its maximum capacity. This alarm should not normally occur when no other congestion alarms are asserted.

2. Application Routing might be mis-configured and is sending too much traffic to the Peer CNDRA Application. Verify the configuration.
3. If no additional congestion alarms are asserted, the Peer CNDRA application task might be experiencing a problem that is preventing it from processing messages from its Request Message Queue. Examine the Alarm log on the active Overseer server.
4. If the problem persists, it is recommended to contact My Oracle Support.

22503 - Peer CNDRA Application Answer Message Queue Utilization

Alarm Group:
APPL

Description:
The Peer CNDRA Application Answer Message Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
<Metric ID>, <Peer CNDRA Application Name>

> **Note:**
>
> The value for Metric ID for this alarm varies (such as RxRbarAnswerMsgQueue) depending on which Peer CNDRA application generates the alarm (such as RBAR). Use the ID that corresponds to the specific Peer CNDRA application in use.

> **Note:**
>
> The value for the Peer CNDRA Application Name varies depending on the Peer CNDRA application generating the alarm (such as RBAR). Use the name that corresponds to the specific Peer CNDRA application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCndraApplicationAnswerQueueUtilNotify

Cause:
Alarm #22503 raises:

- When Peer CNDRA Application AnswerMessage Queue Utilization is approaching its maximum capacity.
- If this problem persists and the queue reaches 100% utilization, all new ingress Answer messages will be discarded.

Diagnostic Information:
To get further information regarding this issue:

1. Examine the alarm log on the active Overseer server.
2. This alarm should not occur when no other congestion alarms are asserted.

1. Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the Peer CNDRA application. Verify the configuration.
2. If no additional congestion alarms are asserted, the Peer CNDRA application task might be experiencing a problem that is preventing it from processing message from its Answer Message Queue. Examine the Alarm log on the active Overseer server.
3. If the problem persists, it is recommended to contact My Oracle Support.

22504 - Peer CNDRA Application Ingress Message Rate

Alarm Group:
APPL

Description:
The ingress message rate for the Peer CNDRA application is exceeding its engineered traffic handling capacity.

Severity:
Minor, Major, Critical

Instance:
<Metric ID>, <Peer CNDRA Application Name>

> **Note:**
>
> The value for metric ID for this alarm varies (such as RxRbarMsgRate) depending on which Peer CNDRA application generates the alarm (such as RBAR). Use the ID that corresponds to the specific Peer CNDRA application in use.

> **Note:**
>
> The value for Peer CNDRA Application Name varies depending on the Peer CNDRA application generating the alarm (such as RBAR, etc.). Use the name that corresponds to the specific Peer CNDRA application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCndraApplicationIngressMsgRateNotify

Cause:
The alarm #22504 raises when the ingress message rate for the Peer CNDRA Application is approaching or exceeding its engineered traffic handling capacity.

This alarm get cleared when the diameter process stops.

Diagnostic Information:
For further information regarding this alarm:

1. Examine the alarm log on Active Overseer Server.
2. Average Ingress Message rate utilization on a MP Server of the Peer CNDRA Application is exceeding or approaching engineering traffic handling capacity.

1. Recovery:

1. Application routing may be mis-configured and is sending too much traffic to the Peer CNDRA application. Verify the configuration.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP.
3. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, it is recommended to contact My Oracle Support.

22520 - Peer CNDRA Application Enabled

Event Type:
APPL

Description:
Peer CNDRA Application Admin state was changed to ‘enabled’.

Severity:
Info

Instance:
<Peer CNDRA Application Name>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterCndraApplicationEnabledNotify

1. Recovery:

- No action required.

22521 - Peer CNDRA Application Disabled

Event Type:
APPL

Description:
Peer CNDRA Application Admin state was changed to ‘disabled’.

Severity:
Info

Instance:
<Peer CNDRA Application Name>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterCndrapplicationDisabledNotify

1. Recovery:

- No action required.

Full Address Based Resolution (FABR) Alarms and Events (22600-22640)

22600 - Message Decoding Failure

Event Type:
FABR

Description:
Message received was rejected because of a decoding failure. While parsing the message, the message content was inconsistent with the "Message Length" in the message header. These protocol violations can be caused by the originator of the

message (identified by the Origin-Host AVP in the message), the peer who forwarded the message to this node, or any intermediate node that modifies the message.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrMsgRejectedDecodingFailureNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22601 - Unknown Application ID

Event Type:
FABR

Description:
Message could not be routed because the Diameter Application ID is not supported. A Request message was forwarded to the FABR application which contained an unrecognized Diameter Application ID in the header. Either an application routing rule is mis-provisioned or the Application ID is not provisioned in the FABR configuration.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrUnknownApplIdNotify

1. Recovery:

1. The currently provisioned Application Routing Rules can be viewed using **Diameter**, and then **Configuration**, and then **Application Route Tables**.
2. The currently provisioned Diameter Application IDs can be viewed in the **FABR**, and then **Configuration**, and then **Applications Configuration**.
3. It is recommended to contact My Oracle Support for assistance.

22602 - Unknown Command Code

Event Type:
FABR

Description:
Message could not be routed because the Diameter Command Code in the ingress Request message is not supported and the Routing Exception was configured to send an Answer response.
Either an application routing rule is mis-provisioned or the Command Code is not provisioned in the FABR configuration.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrUnknownCmdCodeNotify

1. Recovery:

1. The currently provisioned Application Routing Rules can be viewed using **Diameter**, and then **Configuration**, and then **Application Route Tables**.

2. The currently provisioned Diameter Application IDs can be viewed in the **FABR**, and then **Configuration**, and then **Address Resolutions**.
3. It is recommended to contact My Oracle Support for assistance.

22603 - No Routing Entity Address AVPs

Event Type:
FABR

Description:
Message could not be routed because no address AVPs were found in the message and the Routing Exception was configured to send an Answer response.

Severity:
Info

Instance:
<AddrResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrNoRoutingEntityAddrAvpNotify

1. Recovery:
1. If this event is considered abnormal, then validate which AVPs are configured for routing with the Application ID and Command Code using **FABR**, and then **Configuration**, and then **Address Resolutions**.
2. The currently provisioned Application Routing Rules can be viewed using **Diameter**, and then **Configuration**, and then **Application Route Tables**.
3. It is recommended to contact My Oracle Support for assistance.

22604 - No Valid User Identity Addresses Found

Event Type:
FABR

Description:
No valid User Identity Address is found in the configured AVPs contained in the ingress message. FABR searches for a valid Routing Entity address in the ingress Diameter message based on a Routing Entity Preference List assigned to the ordered pair (Application ID, Command Code) via user-defined configuration. This event is raised if a valid Routing Entity address cannot be found using any of the Routing Entity types in the Routing Entity Preference List and if the Routing Exception Action associated with this failure is set to Send Answer response .

Severity:
Info

Instance:
<AddrResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrNoValidUserIdentityAddrFoundNotify

Cause:
FABR searches for a valid Routing Entity address in the Ingress Diameter Message based on a **Routing Entity Preference** List assigned to the ordered pair (Application ID, Command Code) via user-defined configuration. This event raises if a valid **Routing Entity** address cannot be found using any of the **Routing Entity** types in the **Routing Entity Preference** List and if the **Routing Exception Action** associated with this failure is set to **Send Answer Response**.

Diagnostic Information:
Alarm #22604 raises if FABR is unable to decode the user configured AVPS from the **Ingress Diameter Message** and yield a routing entity address. This may be a normal

event or an event associated with mis-provisioned address resolution configuration. If this event is considered abnormal, then the user should validate which AVPs are configured for routing with the Application ID and Command Code using the FABR GUI screen.
The associated measurement tag for this event is **RxFabrResolFailNoValidAddr (10633)**. This holds the number of request messages received with at least Routing Entity Address AVP, but no valid Routing Entity Addresses were found.

1. Recovery:

1. If this event is considered abnormal, then navigate to **FABR**, and then **Configuration**, and then **Address Resolutions** to validate which AVPs are configured for routing with the Application ID and Command Code.
2. Navigate to **Diameter**, and then **Configuration**, and then **Application Route Tables** to view the currently provisioned Application Routing rules.
3. It is recommended to contact My Oracle Support for assistance.

22605 - No Destination address is found to match the valid User Identity address

Event Type:
FABR

Description:
Message could not be routed because the valid user identity address extracted from the message did not resolve to a destination address. The Routing Exception was configured to send an Answer response. Please verify the provisioning in the address resolution table and the data provided in the SDS corresponding to this address/ resolution entry.
The FABR address resolution table entry may be misconfigured or the destination address associated with User Identity address from the message and the destination type configured in the address resolution table may be missing from the address mapping configuration. The destination address associated with User Identity address derived may be missing from the address mapping configuration on DP/SDS.

Severity:
Info

Instance:
<AddrResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrNoAddrFoundAtDpNotify

1. Recovery:

1. Validate the address resolution table entry and verify that a valid destination address is associated with the user identity address by using DP configuration.

For additional information, see Subscriber Database Server online help.

2. It is recommended to contact My Oracle Support for assistance.

22606 - Database or DB connection error

Event Type:
FABR

Description:
FABR application receives service notification indicating Database (DP) or DB connection (ComAgent) Errors (DP timeout, errors or ComAgent internal errors) for the sent database query.

Severity:
Info

Instance:
<MPNname>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrDpErrorsNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22607 - Routing attempt failed due to DRL queue exhaustion

Event Type:
FABR

Description:
Message could not be routed because the internal “Request Message Queue” to the DSR **Relay Agent** was full.

Severity:
Info

Instance:
<MPNname>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrRoutingAttemptFailureDrlQueueExhNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22608 - Database query could not be sent due to DB congestion

Event Type:
FABR

Description:
FABR could not send a database query either because the ComAgent reported DP congestion level of (CL=2 or 3), or an abatement period is in progress.

Severity:
Info

Instance:
<MPNname>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrDpCongestedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22609 - Database connection exhausted

Event Type:
FABR

Description:
Database queries could not be sent because the database connection (ComAgent) queue was full.

Severity:
Info

Instance:
<MPNname>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrDbConnectionExhNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22610 - FABR DP Service congestion state change

Event Type:
FABR

Description:
FABR application received status notification indicating DP congestion state change or DP congestion abatement time period has completed.

Severity:
Info

Instance:
<MPName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterFabrDpCongestionStateChangeNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22611 - FABR Blacklisted Subscriber

Event Type:
FABR

Description:
Message could not be routed because valid User Identity Address extracted from diameter request belongs to blacklisted subscriber.

Severity:
Info

Instance:
<AddrResolution>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterFabrBlacklistedSubscriberNotify

1. Recovery:

1. Validate which User identity address is not blacklisted by using DP configuration.

   The destination address associated with User Identity address derived is blacklisted in the address mapping configuration on DDR.

2. If the problem persists, it is recommended to contact My Oracle Support.

22631 - FABR DP Response Task Message Queue Utilization

Alarm Group:
FABR

Description:
The FABR Application's DP Response Message Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
RxFabrDpResponseMsgQueue, FABR

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterFabrAppDpResponseMessageQueueUtilizationNotify

1. Recovery:

1. This alarm may occur due to persistent overload conditions with respect to database response processing.

2. It is recommended to contact My Oracle Support for assistance.

22632 - ComAgent Registration Failure

Alarm Group:
FABR

Description:
FABR application is unavailable and DSR cannot successfully process FABR traffic.

Severity:
Critical

Instance:
Full Address Based Resolution

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterComAgentRegistFailNotify

Cause:
This alarm is raised when ComAgent fails to register:

- Service with DPService.
  - The DPService routed service entry missing in ComAgent table.
  - FABR routing service has been enabled on the MP blade, but DP routed service entry is not present in the ComAgtRoutedService table on MP blade.
- ServiceNotificationHandler after the successful ComAgent service registration.

Diagnostic Information:

1. Check the ComAgtRoutedService table entries, by running the below command on the MP1 command prompt. iqt -p -s'|' ComAgtRoutedService
2. Entry corresponding to the DP routed service used by FABR must be present with id=11 and name=DPService. For example: 11|DPService|No|Yes|0

1. Recovery:

1. Check the ComAgtRoutedService table entries, by running the below command on the MP1 command prompt.

   ```
   iqt -p -s'|' ComAgtRoutedService
   ```

2. Entry corresponding to the DP routed service used by FABR must be present with id=11 and name=DPService. For example:

   ```
   11|DPService|No|Yes|0
   ```

3. Disable the FABR application to clear the ComAgent Service Registration Failure alarm.
4. Check the ComAgtRoutedService table on NOAM server blade to identify if there is any mismatch with the MP blade.
5. Check the ComAgtRoutedService table on SOAM server blade to identify if there is any mismatch with the MP blade (in case of 3-tier architecture).
6. If DP routed service entry is not present, then add it to the MP blade using the `ivi` command (after turning off the inetrep using `pm.set off inetrep`), then restart the inetrep process.

   Afterwards, please restart the DSR process by running `pm.set off dsr;` followed by `pm.set on dsr;` on MP blade command prompt.
7. It is recommended to contact My Oracle Support for assistance.

Policy and Charging Application (PCA) Alarms and Events (22700-22799)

22700 - Protocol Error in Diameter Requests

Event Group:
PCA

Description:
The Diameter Request message(s) received by PCA contain protocol error(s).

Severity:
Info

Instance:
PCA, <PcaFunctionName>

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraProtocolErrorsInDiameterReqNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22701 - Protocol Error in Diameter Answers

Event Group:
PCA

Description:
The Diameter Answer message(s) received by PCA contain(s) protocol error(s). This error message is based on error scenarios such as:

- Command-Code value is not supported
- Mandatory AVP used for processing decisions is missing
- Mandatory AVP used for processing contains an invalid value
- Mandatory Session-Id AVP has a zero-length value

> **Note:**
>
> This event is not generated when the received Diameter Answer message 'E' (Error) bit is set and a mandatory Diameter command-specific AVP (AVPs other than Session-ID, Origin-Host, Origin-Realm, and result-Code) are missing.

Severity:
Info

Instance:
PCA, <PcaFunctionName>

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraProtocolErrorsInDiameterAnsNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22702 - Database Hash Function Error

Event Type:
PCA

Description:
The hash function result does not map to a database resource or sub-resource.

Severity:
Info

Instance:
N/A

HA Score:
Normal

OID:
pdraPdraHashingResDoesNotMatchResOrSubResNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22703 - Diameter Message Routing Failure Due To Full DRL Queue

Event Type:
PCA

Description:
The Diameter Egress message could not be sent because the DRL Message Queue is full.

Severity:
Info

Instance:
PCA, <PcaFunctionName>

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraEgressMsgRoutingFailureDueToDrlQueueExhaustedNotify

1. Recovery:
1. Refer to measurement RxGyRoAnsDiscardDrlQueueFullPerCmd (in the *DSR Measurements Reference)* to determine the number of Gy/Ro Diameter Credit Control Application Answer messages discarded by OC-DRA due to DRL's Answer queue being full.
2. It is recommended to contact My Oracle Support for assistance.

22704 - Communication Agent Error

Event Type:
PCA

Description:
The Policy and Charging server to SBR server communication failure.

Severity:
Info

Instance:
<PcaFunctionName>

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraStackEventSendingFailureCAUnavailNotify

Cause:
Applicable Diameter Interface/Message Type

- Gx CCR-I, CCR-U and CCR-T
- Rx AAR, STR
- Gx-Prime CCR-I, CCR-U and CCR-T

Diagnostic Information:
Direct Exception Measurement & Measurement Group:

- 10834: **TxPdraErrAnsGeneratedCaFailure** in P-DRA Diameter Exception Measurement Group

3-digit Error Code:

- Refer to EC-507 - Policy SBR Error. ComAgent timeout

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22705 - SBR Error Response Received

Event Type:
PCA

Description:
The Policy and Charging server received response from SBR server indicating SBR errors.

Severity:
Info

Instance:
<PcaFunctionName>

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraPsbrErrorIndicationNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

22706 - Binding Key Not Found In Diameter Message

Event Type:
PCA

Description:
A binding key is not found in the received CCR-I message.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraBindingKeyNotFoundNotify

1. Recovery:

1. Check the P-DRA GUI at **Policy DRA**, and then **Configuration**, and then **Binding Key Priority**.
2. It is recommended to contact My Oracle Support for assistance.

22707 - Diameter Message Processing Failure

Alarm Group:
PCA

Description:
PCA failed to process a Diameter message. The specific reason is provided by the PCA signaling code.

Severity:
Info

Instance:
<PcaFunctionName>

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraDiameterMessageProcessingFailureNotify

1. Recovery:

1. If the event was generated for a Diameter message being discarded due to congestion, refer to the Recovery steps for Alarm 22504 - Peer CNDRA Application Ingress Message Rate.
2. It is recommended to contact My Oracle Support for further assistance.

22708 - PCA Function is Disabled

Alarm Group:
PCA

Description:
The PCA Function is unable to process any messages because it is Disabled.

Severity:
Major

Instance:
<PcaFunctionName>

HA Score:
Normal

Auto Clear Seconds:
60

OID:
pdraPcaFunctionDisabledNotify

1. Recovery:

1. The PCA Function becomes Disabled when the Admin State is set to Disable. The PCA Function Admin State can be determined from the SOAM GUI **Policy and Charging**, and then **General Options**. Verify the admin state is set as expected.
2. If the Admin State of the PCA Function is to remain Disabled, consider changing the ART configuration to stop sending traffic for that function to PCA.
3. It is recommended to contact My Oracle Support for assistance if needed.

22709 - PCA Function is Unavailable

Alarm Group:
PCA

Description:
The PCA Function is unable to process any messages because it is Unavailable.

Severity:
Major

Instance:
<PcaFunctionName>

HA Score:
Normal

Auto Clear Seconds:
0

OID:
pdraPcaFunctionUnavailableNotify

1. Recovery:

1. The availability of the Policy DRA function to receive and process ingress messages is based on its administration state (Enabled or Disabled) and the status of the SBR Binding and Session resources.
2. The availability of the Online Charging DRA function to receive and process ingress messages is based on its administration state (Enabled or Disabled), OCS configuration, and the status of the SBR Session resource.
3. The PCA function is unavailable to receive and process ingress messages for one of the following reasons:
   - "Insufficient Binding SBR Resources" - The number of Binding SBR sub-resources available is less than the minimum number required. Refer to the Recovery steps for Alarm 22722 - Policy Binding Sub-resource Unavailable, which will also be asserted.
   - "Insufficient Session SBR Resources" - The number of Session SBR sub-resources available is less than the minimum number required. Refer to the Recovery steps for Alarm 22723 - Policy and Charging Session Sub-resource Unavailable, which will also be asserted.
   - "No OCSs Configured at Site" - At least one OCS is required to be locally configured. Use the SOAM GUI Main Menu **Policy and Charging**, and then **Configuration**, and then **Online Charging DRA**, and then **OCSs** to configure an OCS at the site.
   - "Session DB has not been created" - A Session SBR Database must be configured for each Policy and Charging Mated Sites Place Association. Use the Network OAM GUI Main Menu **Policy and Charging**, and then **Configuration**, and then **SBR Databases** to configure a Session SBR Database.
   - "Binding DB has not been created" - For P-DRA, a Binding SBR Database must be configured. Use the Network OAM GUI Main Menu **Policy and Charging**, and then **Configuration**, and then **SBR Databases** to configure a Binding SBR Database.
   - "Session DB's admin state is not Enabled" - A Session SBR Database must be Enabled for each Policy and Charging Mated Sites Place Association where signaling is to be processed. Use the Network OAM GUI Main Menu **Policy and Charging**, and then **Maintenance**, and then **SBR Database Status** to Enable a Session SBR Database.
   - "Binding DB's admin state is not Enabled" - For P-DRA, a Binding SBR Database must be Enabled. Use the Network OAM GUI Main Menu **Policy and Charging**, and then **Maintenance**, and then **SBR Database Status** to Enable a Binding SBR Database.
4. It is recommended to contact My Oracle Support for assistance if needed.

22710 - SBR Sessions Threshold Exceeded

Alarm Group:
SBR

Description:
The number of SBR sessions threshold for a Policy and Charging Mated Sites Place Association has been exceeded.

Severity:
Minor, Major, Critical

Instance:
<SbrDatabaseName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrActSessThreshNotify

Cause:
The number of session records stored in the policy session database has exceeded the minor, major, or critical alarm threshold percentage of the calculated session capacity for the topology.

Diagnostic Information:
Check the event or alarm information on the active SOAM and analyze the error trace on this SBR server.

1. Recovery:

1. The session database specified in the Instance field is nearing the limit on the number of session records. Alarm severity is determined by the number of session records stored in the policy session database exceeding the alarm threshold percentage of the calculated session capacity for the topology.
2. If the alarm assert thresholds are improperly configured, they can be configured on a network-wide basis on the NOAM from the **Policy DRA**, and then **Configuration**, and then **Alarm Settings**.
3. In general, the system should be sized to host the expected number of concurrent sessions per policy subscriber.
4. If the system is nearing 100% capacity, it is recommended to contact My Oracle Support for further assistance.

22711 - SBR Database Error

Alarm Group:
SBR

Description:
An error occurred during a SBR database operation.

Severity:
Info

Instance:
<SbrServerType>, <SbrSgNameDbType> (I-SBR)

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterPSBRDbOpFailNotify

1. Recovery:

1. An unexpected, internal error was encountered while the SBR database was being accessed. This error may occur for a variety of reasons:
   a. The database is filled to capacity
   b. Database inconsistency between NO and SO tables caused by a database restore operation. This issue is corrected by the SBR audit.
2. It is recommended to contact My Oracle Support for further assistance.

22712 - SBR Communication Error

Alarm Group:
SBR

Description:
The SBR received an error or timeout response from Communication Agent when sending a stack event to another SBR server.

Severity:
Info

Instance:
<SbrServerType>, <SbrDbType> (I-SBR)

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterPSBRStkEvFailComAgentNotify

1. Recovery:

- It is recommended to contact My Oracle Support for further assistance.

22713 - SBR Alternate Key Creation Error

Alarm Group:
SBR

Description:
Failed to create an Alternate Key record in the Binding database.

Severity:
Info

Instance:
Session SBR

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterPSBRAltKeyCreateFailNotify

1. Recovery:

- It is recommended to contact My Oracle Support for further assistance.

22714 - SBR RAR Initiation Error

Alarm Group:
SBR

Description:
SBR encountered an error while processing PCA initiated RAR requests.

Severity:
Info

Instance:
Session SBR

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterPSBRRARInitiationErrNotify

1. Recovery:

- It is recommended to contact My Oracle Support for further assistance.

22715 - SBR Audit Suspended

Alarm Group:
SBR

Description:
SBR DB (Binding, Session, or Universal) auditing has been suspended because the Session Integrity send rate is more than the engineering configurable threshold, or due to a congestion condition on either the local server reporting the alarm or on a remote server being queried for auditing purposes.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSBRAuditSuspendedNotify

1. Recovery:

1. If the Binding DB server is not locally congested, this alarm indicates that auditing is suspended only on the remote Session servers being queried by Binding for auditing purposes that are congested. The audit cleans up stale records in the database. Prolonged suspension of the audit could result in the exhaustion of memory resources on a binding or session SBR server. Investigate the causes of congestion on the SBR servers (see Alarm 22725 - SBR Server In Congestion).
2. If the problem persists, it is recommended to contact My Oracle Support.

22716 - SBR Audit Statistics Report

Event Group:
SBR

Description:
This report provides statistics related to SBR session or binding table audits. Each SBR server generates this event upon reaching the last record in a table. The statistics reported are appropriate for the type of table being audited. This report also provides hourly statistics related to the Pending RAR report.

Severity:
Info

Instance:
<PcaTableName>, <SbrSgName> (I-SBR)

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterPSBRAuditStatisticsReportNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

22717 - SBR Alternate Key Creation Failure Rate

Alarm Group:
SBR

Description:
SBR Alternate Key Creation Failure rate exceeds threshold.

Severity:
Minor, Major, Critical

Instance:
PsbrAltKeyCreationFailureRate, SBR

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSBRAltKeyCreationFailureRateNotify

1. Recovery:

- If the further assistance is needed, it is recommended to contact My Oracle Support.

22718 - Binding Not Found for Binding Dependent Session Initiate Request

Event Group:
PCA

Description:
Binding record is not found for the configured binding keys in the binding dependent session-initiation request message.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraBindingRecordNotFoundNotify

1. Recovery:

1. Check the Policy and Charging GUI Main Menu **Policy and Charging**, and then **Configuration**, and then **Binding Key Priority** on the subscriber key priorities to ensure the configuration is correct.
2. Using the Binding Key Query Tool, check if a binding exists for the binding keys at **Policy DRA**, and then **Configuration**, and then **Binding Key Priority**.

22719 - Maximum Number of Sessions per Binding Exceeded

Event Group:
PCA

Description:
A Binding capable session initiation request failed because this subscriber already has the maximum number of sessions per binding.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
60

OID:
pdraPdraMaxSessionsReachedNotify

1. Recovery:

1. Determine if the existing sessions are valid. The existing sessions may be displayed using the Binding Key Query Tool to obtain all relevant information including session IDs and PCEF FQDNs.
2. If the sessions exist in the P-DRA but not on the PCEF(s), it is recommended to contact My Oracle Support.

22720 - Policy SBR To PCA Response Queue Utilization Threshold Exceeded

Alarm Group:
PCA

Description:
The SBR to PCA Response Queue Utilization Threshold Exceeded

Severity:
Minor, Major, Critical

Instance:
RxPcaSbrEventMsgQueue, PCA

HA Score:
Normal

OID:
pdraPdraPsbrResponseQueueUtilizationNotify

Auto Clear Seconds:
0 (zero)

1. Recovery:

1. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. Monitor the MP server status from **Status & Manage**, and then **Server Status**
2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP. Monitor the ingress traffic rate of each MP from **Status & Manage**, and then **KPIs**

   Each MP in the server site should be receiving approximately the same ingress transaction per second.
3. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Status & Manage**, and then **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
4. If the problem persists, it is recommended to contact My Oracle Support.

22721 - Policy and Charging Server In Congestion

Alarm Group:
PCA

Description:
The Policy and Charging Server is operating in congestion. Average Policy and Charging ingress messages rate exceeds the configured threshold. The thresholds are based on the engineered system value for Ingress Message Capacity.

Severity:
Minor, Major, Critical

Instance:
PCA

HA Score:
Normal

OID:
pdraPdraCongestionStateNotify

Auto Clear Seconds:
0 (zero)

Cause
This alarm raises when the Average Policy and Charging ingress messages rate exceeds the configured threshold. The thresholds are based on the engineered system value for Ingress Message Capacity.

Diagnostic Information:

- The alarm thresholds for **DSR Application Ingress Message Rate** are configured network wide on Network OAM using the **Policy DRA > Configuration > Alarm Settings** and **Congestion Options** screens.
- Monitor the ingress traffic rate of each MP by selecting **Main Menu > Status & Manage > KPIs**. If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.

1. Recovery:

1. Adjust the alarm threshold parameters. Verify the configuration by navigating to the Congestion Options on **Policy DRA**, and then **Configuration**, and then **Alarm Settings**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Status & Manage**, and then **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, it is recommended to contact My Oracle Support.

22722 - Policy Binding Sub-resource Unavailable

Alarm Group:
PCA

Description:
One or more Policy binding sub-resources are not available.

Severity:

- Major: When a Binding SBR Database is prepared or enabled and at least one server group that has a range of binding sub-resources is not available
- Critical: When a Binding SBR Database is prepared or enabled and all of the binding sub-resources are not available, i.e., all server groups hosting the sub-resources are not available.

Instance:
<ResourceDomainName>

HA Score:
Normal

OID:
pdraPdraBindingSubresourceUnavailableNotify

Auto Clear Seconds:
0 (zero)

1. Recovery:

1. At the NOAM, navigate to the SBR Database Status screen at **Policy and Charging**, and then **Maintenance**, and then **SBR Database Status** and locate the SBR Database specified in the Alarm Additional Information. The database's Operational Status and the Operational Reason values associated with resource users and resource providers are displayed.
2. Click on the row for the Database Name. If the Resource User Operational Reason has a colored cell, the lower-left pane on the status screen will display information about which resource users are having problems accessing the database. If the Resource Provider Operational Reason has a colored cell, the lower-right pane on the status screen will display information about which resource providers are unable to provide service.
3. If the Resource Provider pane on the lower right is empty, look for ComAgent connection Alarms. If ComAgent connection alarms exist, follow the Recovery steps for those alarms to troubleshoot further. If there are no ComAgent connection alarms, review the configuration of Resource Domains, Places, and Place Associations using the NOAM GUI and verify that they are provisioned as expected:
   - **Configuration**, and then **Resource Domains**
   - **Configuration**, and then **Places**
   - **Configuration**, and then **Place Associations**
4. Click the Database Name hyperlink to go to the SBR Database Configuration View screen, filtered by the SBR Database Name. Make note of the Resource Domain configured for the SBR Database.
5. Navigate to the ComAgent HA Services Status screen at **Communication Agent**, and then **Maintenance**, and then **HA Service Status** and locate the Resource with name equal to that configured as the Resource Domain for the SBR Database.
6. Click the HA Services Status row for the Resource, which will have further detailed information about the Communication Agent's problem.
7. It is recommended to contactMy Oracle Support for assistance if needed.

22723 - Policy and Charging Session Sub-resource Unavailable

Alarm Group:
PCA

Description:
One or more Policy and Charging session sub-resources are not available.

Severity:

- Major: When a Session SBR Database is prepared or enabled and at least one of the server groups hosting session sub-resources is not available.

- Critical: When a Session SBR Database is prepared or enabled and all of the server groups hosting session sub-resources are not available.

Instance:
<ResourceDomainName>

HA Score:
Normal

OID:
pdraPdraSessionSubresourceUnavailableNotify

Auto Clear Seconds:
0 (zero)

1. Recovery:

1. At the NOAM, navigate to the SBR Database Status screen at **Policy and Charging**, and then **Maintenance**, and then **SBR Database Status** and locate the SBR Database specified in the Alarm Additional Information. The database's Operational Status and the Operational Reason values associated with resource users and resource providers are displayed.
2. Click on the row for the Database Name. If the Resource User Operational Reason has a colored cell, the lower-left pane on the status screen will display information about which resource users are having problems accessing the database. If the Resource Provider Operational Reason has a colored cell, the lower-right pane on the status screen will display information about which resource providers are unable to provide service.
3. If the Resource Provider pane on the lower right is empty, look for ComAgent connection Alarms. If ComAgent connection alarms exist, follow the Recovery steps for those alarms to troubleshoot further. If there are no ComAgent connection alarms, review the configuration of Resource Domains, Places, and Place Associations using the NOAM GUI and verify that they are provisioned as expected:
   - **Configuration**, and then **Resource Domains**
   - **Configuration**, and then **Places**
   - **Configuration**, and then **Place Associations**
4. Click the Database Name hyperlink to go to the SBR Database Configuration View screen, filtered by the SBR Database Name. Make note of the Resource Domain configured for the SBR Database.
5. Navigate to the ComAgent HA Services Status screen at **Communication Agent**, and then **Maintenance**, and then **HA Service Status** and locate the Resource with name equal to that configured as the Resource Domain for the SBR Database.
6. Click the HA Services Status row for the Resource, which will have further detailed information about the Communication Agent's problem.
7. It is recommended to contact My Oracle Support for assistance if needed.

22724 - Policy SBR Memory Utilization Threshold Exceeded

Alarm Group:
SBR

Description:
The SBR server memory utilization threshold has been exceeded.

Severity:
Minor, Major, Critical

Instance:
Policy and Charging mated Sites Place Association Name

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrMemUtilNotify

Cause:
Policy pSBR server memory utilization threshold has been exceeded.
This alarm's assert conditions are defined by the following default parameters:

- **Minor:** pSBR memory utilization threshold > 70%
- **Major:** pSBR memory utilization threshold > 80%
- **Critical:** pSBR memory utilization threshold > 90%

Diagnostic Information:

- The pSBR exceeds the engineered memory utilization levels.
- Do not rasie pSBR memory Alarm 22724 on non-pSBR servers.
- Check the server memory usage.

1. Recovery:

1. Change threshold parameters.
2. If this condition persists, it may be necessary to allocate more memory for pSBR.
3. It is recommended to contact My Oracle Support for further assistance.

22725 - SBR Server In Congestion

Alarm Group:
SBR

Description:
The SBR server is operating in congestion.

Severity:

- Minor: CL_1
- Major: CL_2
- Critical: CL_3

Instance:
Policy and Charging mated Sites Place Association Name, <SbrSgName> (I-SBR)

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrServerInCongestionNotify

1. Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter**, and then **Configuration**, and then **Application Route Tables**.
2. There may be an insufficient number of MPs configured to handle the network load. Monitor the ingress traffic rate of each MP by selecting **Status & Manage**, and then **KPIs**.

   If MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. If the problem persists, it is recommended to contact My Oracle Support.

22726 - SBR Queue Utilization Threshold Exceeded

Alarm Group:
SBR

Description:
The SBR stack event queue utilization threshold has been exceeded. The alarm is asserted for three separate stack event queues (PsbrSisTaskQMetric, PsbrSisSendRarTaskQMetric, and PsbrInvokeSisRspHandlerTaskQMetric) in Binding and Session SBR servers.

Severity:
Minor, Major, Critical

Instance:
SBR

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrStackEvQUtilNotify

Cause:
The alarm is asserted for the separate stack event queues as following:

- PsbrBindingTaskQMetric
- PsbrSessionTaskQMetric
- PsbrAuditStackEventTaskQMetric
- PsbrTableWatcherTaskQMetric
- PsbrSisTaskQMetric
- PsbrSisSendRarTaskQMetric
- PsbrInvokeSisRspHandlerTaskQMetric
- PsbrSisRspHandlerTaskQMetric

Each stack event queue has its configurable threshold parameters.
Default values as following:

- Assert conditions:
  - **Minor:** pSBR stack event queue utilization threshold > 80%
  - **Major:** pSBR stack event queue utilization threshold > 90%
  - **Critical:** pSBR stack event queue utilization threshold > 100%
- Clear conditions:
  - **Minor:** pSBR stack event queue utilization threshold <= 70%
  - **Major:** pSBR stack event queue utilization threshold <= 85%
  - **Critical:** pSBR stack event queue utilization threshold <= 95%

Diagnostic Information:
To further diagnose the issue:

- Check the event/alarm information on the active SOAM and analyze the error trace on this SBR server.
- Collect Savelogs on this SBR server.
- Event History on the active SOAM server.

1. Recovery:

- If this condition persists, collect the Savelogs under Diagnostic information on the SBR server and it is recommended to contact My Oracle Support for further assistance.

22727 - SBR Initialization Failure

Alarm Group:
SBR

Description:
The SBR server process failed to initialize.

Severity:
Critical

Instance:
Policy DRA Mated Sites Place Association Name

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrInitializationFailureNotify

Cause:

- Any of the ComAgent registration calls for either session resource or binding resource fails during the pSBR initialization.
- Unable to calculate the number of Session or Binding Sub-resource.
- Unable to initialize the SBR internal resource. For example, PsbrHaMgr.

Diagnostic Information:

- Check the event/alarm information on the active SOAM and analyze the error trace on this SBR server.
- Collect Savelogs on this SBR server.
- Event history on the active SOAM server.

1. Recovery:

- If this condition persists, collect the Savelogs under Diagnostic information on the SBR server and it is recommended to contact My Oracle Support for further assistance

22728 - SBR Bindings Threshold Exceeded

Alarm Group:
SBR

Description:
The number of bindings threshold has been exceeded.

Severity:
Minor, Major, Critical

Instance:
<SbrDatabaseName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrActBindThreshNotify

Cause:
The Binding Region specified in the Instance field is nearing the expected number of binding records for this network.

Diagnostic Information:
The alarm thresholds for Binding Capacity alarms are configured network wide on Network OAM using the "Policy DRA > Configuration > Alarm Settings" screen.

- If the alarm severity is minor, the alarm means that the number of binding records stored in Binding Region has exceeded the minor alarm threshold percentage of the calculated binding capacity for the topology.
- If the alarm severity is major, the alarm means that the number of binding records stored in Binding Region has exceeded the major alarm threshold percentage of the calculated binding capacity for the topology.
- If the alarm severity is major, the alarm means that the number of binding records stored in Binding Region has exceeded the major alarm threshold percentage of the calculated binding capacity for the topology.

1. Recovery:

1. The binding database specified in the Instance field is nearing the limit on the number of binding records. The alarm threshold percentages can be modified as desired by the network operator at the NOAM using **Policy and Charging**, and then **Configuration**, and then **Alarm Settings**.
2. If a given alarm severity is unwanted, the alarm severity may be suppressed by checking the Suppress checkbox for that alarm severity.
3. It is recommended to contact My Oracle Support to discuss plans for system growth is this alarm continues to be asserted under normal operating conditions.

> **Note:**
>
> It is expected, but not guaranteed, that the system will continue to function beyond the tested maximum number of subscribers with bindings.

22729 - PCRF Not Configured

Alarm Group:
PCA

Description:
PCRF Not Configured

Severity:
Major

Instance:
Policy Binding Region Place Association Name

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
pdraPcrfNotConfiguredNotify

Cause:
This alarm raises when the P-DRA completes initialization and determines that the PCRF's are not configured.

Diagnostic Information:

- Check the NOAM GUI at **Main Menu > Policy and Charging > Configuration > Policy DRA** for further PCRF configuration.
- Check for any missing configuration or capture this screen for further analysis.

1. Recovery:

1. Check the NOAM GUI at **Policy and Charging**, and then **Configuration**, and then **Policy DRA** for further PCRF configuration.
2. Check the event history logs in **Alarms & Events**.
3. If the problem persists, it is recommended to contact My Oracle Support.

22730 - Policy and Charging Configuration Error

Alarm Group:
PCA

Description:
Policy and Charging message processing could not be successfully completed due to a configuration error.

Severity:
Major

Instance:
<ConfigurationError>

HA Score:
Normal

OID:
pdraPdraConfigErrorNotify

Auto Clear Seconds:
300 (5 minutes)

Cause:

- The session initiation request message was received with a missing or un-configured APN.

- Binding capable session initiation answers was coming from an unconfigured PCRF.
- The binding independent session initiation request was routed to an OCS that is not configured.

Diagnostic Information:

- Check DSR configuration
- Check Diameter message PCAP.

1. Recovery:

1. If there is an unconfigured PCRF, it means the binding capable session initiation request was routed to a PCRF that is not configured in **Policy and Charging**, and then **Configuration**, and then **Policy DRA**, and then **PCRFs** at the site where the request was received. This indicates a mismatch between the PCRF's configuration and the routing configuration. If the PCRF is a valid choice for the request, configure the PCRF in **Policy and Charging**, and then **Configuration**, and then **Policy DRA**, and then **PCRFs**. If the PCRF is not valid for the request, correct the routing table or tables included the PCRF.

   Also see measurement RxBindCapUnknownPcrf in the DSR Measurement Reference.

2. If there is an unconfigured APN and if the APN string is valid, configure the APN at the NOAM using the **Policy and Charging**, and then **Configuration**, and then **Access Point Names** screen. If the APN string is not valid, investigate the policy client to determine why it is sending policy session initiation requests using the invalid APN.

   Also see measurements RxBindCapUnknownApn and RxBindDepUnknownApn in the *DSR Measurement Reference*.

3. If there is a missing APN, investigate the policy client to determine why it is sending policy session initiation requests with no APN.

   Also see measurements RxBindCapMissingApn and RxBindDepMissingApn in the *DSR Measurement Reference*.

4. If there are no PCRFs configured, configure PCRFs at the SOAM GUI for the site using **Policy and Charging**, and then **Configuration**, and then **PCRFs**.

5. If there is an unconfigured OCS, it means that the binding independent session initiation request was routed to an OCS that is not configured in **Policy and Charging**, and then **Configuration**, and then **Online Charging DRA**, and then **OCSs**. This indicates a mismatch between the OCSs configuration and the routing configuration. If the OCS named in the alarm additional information is a valid choice for the request, configure the OCS at the SOAMP using **Policy and Charging**, and then **Configuration**, and then **Online Charging DRA**, and then **OCSs**. If the OCS is not valid for the request, correct the routing table or tables included the OCS.

6. It is recommended to contact My Oracle Support.

22731 - Policy and Charging Database Inconsistency

Alarm Group:
PCA

Description:
The Policy and Charging database inconsistency exists due to an internal data error or internal database table error.

Severity:
Major

Instance:
<PcaFunctionName>

HA Score:
Normal

Auto Clear Seconds:
60

OID:
pdraPdraDbInconsistencyExistsNotify

1. Recovery:

1. Check the error history logs for the details of the data inconsistency.
2. If the problem persists, it is recommended to contact My Oracle Support.

22732 - SBR Process CPU Utilization Threshold Exceeded

Alarm Group:
SBR

Description:
The SBR process on the indicated server is using higher than expected CPU resources.

Severity:
Minor, Major, Critical

Instance:
psbr.cpu, SBR

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrProcCpuThreshNotify

Cause:
Policy SBR Process CPU Utilization Threshold has been exceeded. The Policy SBR process on the indicated server is using higher than expected CPU resources.

Diagnostic Information:
This alarm's assert conditions are defined by the following parameters:

- **Minor**: pSBR process CPU utilization threshold > 60%
- **Major**: pSBR process CPU utilization threshold > 66%
- **Critical**: pSBR process CPU utilization threshold > 72%

See the alarm history of the event for the current CPU utilization. Ensure that the utilization is less than the threshold values

1. Recovery:

1. If this condition persists, it may be necessary to deploy more policy signaling capacity.
2. It is recommended to contact My Oracle Support for further assistance.

22733 - SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration

Alarm Group:
SBR

Description:
The SBR failed to free binding memory after PCRF Pooling binding migration.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSBRPostMigrationMemFreeNotify

1. Recovery:

1. On systems upgraded from a release where Policy DRA was running, but that did not support PCRF Pooling, to a release that supports PCRF Pooling, binding data is migrated from the tables used by the old release to tables used by the new release. Once this migration process completes on a given binding policy SBR, a script is automatically executed to free memory for the old tables. If this script should fail for any reason to free the memory, this alarm is asserted.
2. If additional assistance is needed, it is recommended to contact My Oracle Support.

22734 - Policy and Charging Unexpected Stack Event Version

Alarm Group:
PCA

Description:
A Policy and Charging server received a stack event with an unexpected down-version.

Severity:
Major

Instance:
N/A

HA Score:
Normal

OID:
pdraPdraUnexpectedSEDownVersionNotify

Auto Clear Seconds:
300 (5 minutes)

Cause:
A Policy and Charging server received a stack event with an unexpected down-version. One of the SBRs is running on an older version of DSR software.

Diagnostic Information:
From the event history, view the details of this alarm. Determine which server/server group the alarm was raised for.

1. Recovery:

1. From the NOAM GUI at **Policy and Charging**, and then **Maintenance**, and then **SBR Status**, find the Resource Domain Name to which the stack event was being sent.
2. Expand all Server Groups having that Resource Domain name to see which Server Group hosts the ComAgent Sub Resource.
3. The Server with Resource HA Role of "Active" is likely the server that has the old software (unless a switch-over has occurred since the alarm was asserted). In any case, one of the servers in the Server Group has old software. The software version running on each server can be viewed from **Administration**, and then **Upgrade**. The "Hostname" field is the same as the Server Name on the SBR Status screen
4. Find the server or servers running the old software and upgrade those servers to the current release and accept the upgrade.
5. If additional assistance is needed, it is recommended to contact My Oracle Support.

22735 - Policy DRA session initiation request received with no APN

Event Group:
PDRA

Description:
A Policy DRA session initiation request was received with no APN.

Severity:
Info

HA Score:
Normal

Instance:
None

Throttle Seconds:
30

OID:
pdraPdraSessInitReqWithNoApnNotify

1. Recovery:

1. Investigate why the policy client named by the Origin-Host FQDN in the additional information field is not including the Called-Station-ID AVP and correct it to include the APN.
2. Investigate why the policy client named by the Origin-Host FQDN in the additional information field is not including the Called-Station-ID AVP and correct it to include the APN. Or have that policy client include another binding correlation key that can be used to find the binding
3. Examine associated measurements RxBindCapMissingApn and RxBindDepMissingApn (refer to the *DSR Measurements Reference* for details about these measurements).
4. If the problem persists, it is recommended to contact My Oracle Support.

22736 - SBR failed to free shared memory after a PCA function is disabled

Alarm Group:
SBR

Description:
SBR failed to free shared memory after a PCA function is disabled

Severity:
Minor

HA Score:
Normal

Instance:
<PcaFunctionName>

Auto Clear Seconds:
0 (zero)

OID:
pdraPSBRPostPcaFunctionDisableMemFreeNotify

1. Recovery:

- If the problem persists, it is recommended to contact My Oracle Support.

22737 - Configuration Database Not Synced

Alarm Group:
PCA

Description:
Configuration Database is not synced between the System OAM and Network OAMP.

Severity:
Minor

Instance:
Site name of SOAM server which asserted this alarm

HA Score:
Normal

OID:
pdraPcaConfDbNotSyncedNotify

Auto Clear Seconds:
0 (zero)

1. Recovery:

1. Make note of all **Status & Manage**, and then **Database Resote** operations (if any) at NOAM or SOAM within a day of the occurrence of alarm.
2. Gather all configuration changes (Insert, Edit, or Delete) for PCRFs, Policy Clients, OCSs, CTFs via Security Log from the time the database restore was executed until the present. If there was no database restore performed, then start from the time the alarm was first asserted until the present.
3. If additional assistance is needed, it is recommended to contact My Oracle Support.

22738 - SBR Database Reconfiguration State Transition

Event Group:
SBR

Description:
This event is generated any time a state transition occurs in a SBR Database Resizing or Data Migration Plan. This includes both state transitions due to a user clicking a button on the SBR Database Reconfiguration Status screen and internal state transitions.

Severity:
Info

Instance:
<SbrReconfigurationPlanName>, <SbrReconfigurationPlanName> (I-SBR)

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterPsbrReconfigStateTransitionNotify

1. Recovery:

- This event records the time and conditions under which an SBR Database Reconfiguration Plan (identified in the event instance field) undergoes a state transition. The event additional information includes details such as the previous state, current state, and whether the "Force" option was chosen. This event can be used to obtain a timeline of the entire history of a given reconfiguration plan.

22740 - SBR Reconfiguration Plan Completion Failure

Alarm Group:
SBR

Description:
Failed to successfully complete an SBR Reconfiguration Plan.

> **Note:**
>
> When an SBR Reconfiguration Plan is completed by the user clicking **Complete**, or **Force Complete** on the SBR Reconfiguration Status GUI, database updates are performed to finalize the reconfiguration plan as follows. If any of these updates fail, this alarm shall be asserted.
>
> - Condition 1: Failed to update the Resource Domain of the SBR Database to point to the Target Resource Domain of the Resizing Plan on completion of a Resizing Plan.
> - Condition 2: Failed to mark the Initial SBR Database so that it is no longer the default database for the Place Association on completion of a Data Migration Plan.
> - Condition 3: Failed to mark the Target SBR Database as the default database for the Place Association on completion of a Data Migration Plan.
> - Condition 4: Failed to enable the Target SBR Database on completion of a Data Migration Plan.
> - Condition 5: Failed to disable the Initial SBR Database on completion of a Data Migration Plan.

Severity:

- Minor: Condition 5

- Critical: Conditions 1-4

Instance:
<SbrReconfigPlanAndCondition>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPSbrReconfigConditionsErrorNotify

1. Recovery:

- The SBR Reconfiguration plan specified in the Alarm Instance was not successfully completed, possibly leaving the SBR Database in an abnormal state. Make note of the specific reason for the alarm, and it is recommended to contact My Oracle Support for assistance.

22741 - Failed to route PCA generated RAR

Event Group:
PCA

Description:
Unable to Route RAR generated at PCA

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterPcaGeneratedRARRouteErrNotify

1. Recovery:

- Use Destination-Host to identify the locally generated RAR routing failures and correct the respective configurations. If the DRL provides an error message, it will be displayed with this event, which will have a 3-digit internal error code.

22742 - Enhanced Overload Control AdminState Mismatch

Event Type
PCA

Description
Enhanced Overload Control administrative and operational states are mismatched.

Severity
Major

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterEnhancedOverloadCtrlAdminStateMismatch

1. Recovery

- A change of the Enhanced Overload Control mode configuration (from Enable to Disable or vice versa) requires DA-MPs and/or SBR MPs restarted withing the NO. Verify if the relevant servers are restarted intended by the EOC Mode configuration.

22743 - PCA Server Congested Due to Composite Resource Congestion

Event Type
PCA

Description
PCA Server Congested Due to Composite Resource Congestion.

Severity
Minor, Major, Critical

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterPcaCongrestionStateNotify

1. Recovery
   The PCA server is congested because at least one of the PCA resources is congested.

1. The Application Routing Table may be configured incorrectly and too much traffic was sent to PCA. Verify the configuration via **Diameter**, and then **Configuration**, and then **Application Routing Rules**.

2. A burst of ingress traffic from the network. There may be insufficient number of DA-MPs configured to handle the network load. The ingress traffic rate of each DA-MP can be monitored from **Status & Manage**, and then **KPIs**. If DA-MPs are in a congestion state, then the offered load to the server site is exceeding its capacity.
3. It is recommended to contact My Oracle Support for assistance if needed.

22750 - Enhanced Suspect Binding Removal Feature Enabled

Event Group:
SBR

Description:
The Enhanced Suspect Binding Feature is enabled.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterEnhSuspBindingFeatEnabledNotify

1. Recovery:

- No action required.

22751 - Binding Audit Suppression by Suspect Binding Removal

Alarm Group:
SBR

Description:
The binding SBR audit function is suppressed by the Enhanced Suspect Binding Removal feature.

Severity:
Minor

Instance:
PCA

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
Recovery:

1. If this condition persists, it may indicate a failure of a PCRF or the need to change the configuration of the Suspect Binding Removal Rules.
2. It is recommended to contact My Oracle Support for further assistance.

22752 - SBR Process Not Running

Alarm Group:
SBR

Description:
A managed SBR process cannot be started or has unexpectedly terminated.

Severity:
Major

Instance:
xxx

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
xxx

1. Recovery:

- It is recommended to contact My Oracle Support for further assistance.

SCEF (23000-23200, 102801-115001, 390000)

This section provides information and recovery procedures for SCEF alarms, which range from 23000-23200, 102801-115001, and 390000.

23150 - Diameter Application Not Supported

Event Type:
SCEF

Description:
Diameter message received was not processed as it contained an unsupported Application Identifier.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23152 - Universal SBR Sub-Resource Unavailable

Alarm Group:
SCEF

Description:
One or more Universal SBR sub-resources are unavailable

Severity:
Critical, Major

Instance:
<ResourceDomainName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
scefUsbrSubresourceUnavailableNotify

Cause:
This alarm is cleared if any of the following conditions are met:

- When a relevant Universal SBR Database administrative state is Disable and the Operational Status is Providers Detaching or Disable
- When a relevant Universal SBR Reconfiguration Plan administrative state is Cancel and the Operational Status is Providers Detaching From Target and the resource user has received notification (from ComAgent) that all of the initial sub-resources are available
- When a relevant Universal SBR Reconfiguration Plan administrative state is Complete and the Operational Status is Providers Detaching From Initial and the resource user has received notification (from ComAgent) that all of the target sub-resources are available
- The application process (dsr) on the server that asserted the alarm is shut down
- The SCEF application on the server that asserted the alarm is manually Disabled

Diagnostic Information:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23153 - Diameter Command Code not supported

Event Type:
SCEF

Description:
Diameter message received was not processed as it contained an unsupported Command Code.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23154 - HTTP Message Processing Error

Event Type:
SCEF

Description:
HTTP message received could be processed due to an error.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23155 - SCEF Configuration Error

Alarm Group:
SCEF

Description:
Message processing failed because a required configuration was not found.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
300

OID:
scefConfigurationErrorNotify

Cause:
This alarm is triggered by a transient condition (for example, receipt of an ingress message) and is cleared automatically <Auto Clear Secs> after the last time the condition occurs.

Diagnostic Information:
N/A

1. Recovery:

- No action required.

23156 - Protocol Error in Diameter Message

Event Type:
SCEF

Description:
Diameter message received was not processed due to protocol errors.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23157 - Protocol Error in HTTP Message

Event Type:
SCEF

Description:
HTTP message received was not processed due to protocol errors.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23158 - Universal SBR Error

Event Type:
SCEF

Description:
SCEF-MP server received an error response from the Universal SBR server.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23159 - Diameter Request Routing Failure

Event Type:
SCEF

Description:
Diameter request could not be routed by the local Diameter Stack.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- It is recommended to contact My Oracle Support for assistance.

23160 - Access Control Not Enabled

Alarm Group:
SCEF

Description:
This event is raised when ACL is not configured for SCS.

Severity:
Info

Instance:
ScsAsId

Auto Clear Seconds:
86400

1. Recovery:

- Configure ACL for ScsAs by adding the entry to the ScefACL table and associating the same with ScsAs.

23161 - USBR Response Queue Utilization Threshold Exceeded

Alarm Group:
SCEF

Description:
This event is raised each time queue utilization for USBR response task exceeds the configured threshold value.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
300

1. Recovery:

- If this event is observed consistently, monitor alarms/events raised in USBR.

23162 - Polling Event Queue Utilization Threshold Exceeded

Alarm Group:
SCEF

Description:
This event is raised each time queue utilization for SCEF polling task exceeds the configured threshold value.

Severity:
Major

Instance:
None.

HA Score:
Normal

Auto Clear Seconds:
300

1. Recovery:

- If this event is observed consistently, there may be too many concurrent events received for same subscriber. Monitor the USBR alarms and measurements to identify issue.

102801 -

Event Type:
SCEF

Description:
An alarm was raised from the policy rule file.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Recovery:
1. Investigate using the log for stacktrace.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102826 -

Event Type:
SCEF

Description:
The application does not exist or it is in an inactive state.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Recovery:
1. Create an application instance if one does not exist
2. Make the application active if the state is inactive.

3. It is recommended to contact My Oracle Support if further assistance is needed.

102827 -

Event Type:
SCEF

Description:
The service provider or application cannot be resolved.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Make sure the service provider and application account exist.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102828 -

Event Type:
SCEF

Description:
The request rate is higher than the rate stated in the Service Level Agreement for the service type.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102829 -

Event Type:
SCEF

Description:
The quota for the service type stated in the Service Level Agreement is exceeded.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102830 -

Event Type:
SCEF

Description:
Properties from application are not allowed.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider of the application behavior.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102831 -

Event Type:
SCEF

Description:
The value from a parameter in the application is not allowed.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider of the application behavior or update the SLA to allow the parameter value.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102832 -

Event Type:
SCEF

Description:
The RequestInfo object is empty and cannot proceed with the request.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Check the logs.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102833 -

Event Type:
SCEF

Description:
An application tried to use a method that is not allowed according to the SLA.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102834 -

Event Type:
SCEF

Description:
An application tried to use a method that is not allowed according to the SLA.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102835 -

Event Type:
SCEF

Description:
A service correlator threw an exception when it was invoked.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Examine log files.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102836 -

Event Type:
SCEF

Description:
The RequestFactory threw an exception when it was invoked.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Examine log files.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102837 -

Event Type:
SCEF

Description:
Could not find a global node or service provider node SLA.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Update the node SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102838 -

Event Type:
SCEF

Description:
The service contract in the SLA for the service provider group or application group has expired.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102839 -

Event Type:
SCEF

Description:
The application or service provider group service type contract is out of date. The service contract for the service type in the SLA for the service provider group or application group has expired.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102840 -

Event Type:
SCEF

Description:
The service contract for the service type in the SLA for the service provider group or application group could not be found.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102844 -

Event Type:
SCEF

Description:
The application or service provider group within the service contract has expired.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102845 -

Event Type:
SCEF

Description:
The request rate is higher than the rate specified in the composed service contract.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

102846 -

Event Type:
SCEF

Description:
The quota for the composed service contract has been exceeded.

Severity:
Major

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Notify the service provider or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

111007 -

Event Type:
SCEF

Description:
The value of the budget is below 20% of the maximum value.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Inform the service provider that the request limit is closing or update the SLA.
2. It is recommended to contact My Oracle Support if further assistance is needed.

115001 -

Event Type:
SCEF

Description:
An SLA is about to expire.

Severity:
Warning

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. Check the SLA's valid period.
2. It is recommended to contact My Oracle Support if further assistance is needed.

390000 -

Event Type:
SCEF

Description:
An incoming request violated a firewall policy.

Severity:
Warning

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
###

OID:
N/A

1. This is a security alert, rather than a Services Gatekeeper problem. The action you take depends on your security policies.
2. It is recommended to contact My Oracle Support if further assistance is needed.

Tekelec Virtual Operating Environment, TVOE (24400-24499)

This section provides information and recovery procedures for the Tekelec Virtual Operation Environment (TVOE) alarms, ranging from 24400-24499.

24400 - TVOE libvirtd is down

Alarm Group:
TVOE

Description:
This alarm indicates that the libvirtd daemon is not running.

Severity:
Major

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
1.3.6.1.4.1.323.5.3.31.1.1.2.1

Alarm ID:
TKSTVOEMA1

1. Recovery:

- If the problem persists, it is recommended to contact My Oracle Support.

24401 - TVOE libvirtd is hung

Alarm Group:
TVOE

Description:
This alarm indicates that we attempted to determine if the libvirtd daemon is not responding and it did not respond.

Severity:
Major

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
1.3.6.1.4.1.323.5.3.31.1.1.2.2

Alarm ID:
TKSTVOEMA2

1. Recovery:

- If the problem persists, it is recommended to contact My Oracle Support.

24402 - all TVOE libvirtd connections are in use

Alarm Group:
TVOE

Description:
This alarm indicates that all twenty connections to libvirtd are in use and more could be killed.

Severity:
Major

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
1.3.6.1.4.1.323.5.3.31.1.1.2.3

Alarm ID:
TKSTVOEMA3

1. Recovery:

- If the problem persists, it is recommended to contact My Oracle Support.

Computer Aided Policy Making, CAPM (25000-25499)

This section provides information and recovery procedures for the Computer-Aided Policy Making (CAPM) feature (i.e., Diameter Mediation) alarms and events, ranging from 25000 - 25499, and lists the types of alarms and events that can occur on the system. All events have a severity of Info.

Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the **Alarms & Events**, and then **View History** page.

25000 - CAPM Update Failed

Event Type:
CAPM

Description:
The Rule Template failed to update because of syntax errors. The Additional Info of the Historical alarm includes the name of the Rule Template that failed to be updated.

When the alarm is caused by CAPM Rule Template which contains a syntax error, it may not be raised immediately after applying the template, but may occur when the first Rule has been provisioned and committed.

Severity:
Minor

Instance:
<ruleset> or <ruleset:rule-id>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCapmUpdateFailedNotify

1. Recovery:

1. Check the CAPM Rule Template and verify that the left-hand side term of each condition contains a valid Linking-AVP or Select expression.

   A typical problem can be a non-existing expression, or syntax error of a custom-defined Select expression. If the CAPM Rule Template contains a syntax error, create a new Rule Template by copying and modifying the existing one, then deleting the old Rule Template.

2. Verify also that the recently provisioned data of the Rule Template does not contain a syntax error, i.e., the regular expressions are correct, the fields expecting numbers contain only numbers, etc.

25001 - CAPM Action Failed

Event Type:
CAPM

Description:
When a new Rule Template is created, a failure occurs when performing the action.

Severity:
Info

Instance:
<ruleset> or <ruleset:rule-id>

HA Score:
Normal

Throttle Seconds:
30

OID:
eagleXgDiameterCapmActionFailedNotify

1. Recovery:

- Check the reasons the action failed. It may be a lack of system resources to perform an action, or the action may refer to a part of the message that is not available.

25002 - CAPM Exit Rule Template

Event Type:
CAPM

Description:
When Action Error Handling is set to ‘immediately exit from the rule template’ for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped.

Severity:
Info

Instance:
<ruleset> or <ruleset:rule-id>

HA Score:
Normal

Throttle Seconds:
30

OID:
eagleXgDiameterCapmExitRuleFailedNotify

1. Recovery:

- No action required.

25003 - CAPM Exit Trigger

Event Type:
CAPM

Description:
When Action Error Handling is set to ‘immediately exit from the trigger point’ for the given Rule Template and a failure occurs when performing the action, processing of the Rule Template is stopped (subsequent templates within the trigger point are also skipped).

Severity:
Info

Instance:
<ruleset> or <ruleset:rule-id>

HA Score:
Normal

Throttle Seconds:
30

OID:
eagleXgDiameterCapmExitTriggerFailedNotify

1. Recovery:

- No action required.

25004 - Script failed to load

Alarm Type:
CAPM

Description:
Script syntax error

Severity:
Minor

Instance:
<script name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterCapmScriptLoadingFailedNotify

1. Recovery:

- Check for syntax errors in the script

25005 - CAPM Generic Event

Event Type:
CAPM

Description:
CAPM Generic Event

Severity:
Info

Instance:
<template-id:rule-id>

HA Score:
Normal

Throttle Seconds:
30

OID:
eagleXgDiameterCapmGenericInfoAlarmNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

25006 - CAPM Generic Alarm - Minor

Event Type:
CAPM

Description:
CAPM Generic Alarm - Minor

Severity:
Minor

Instance:
<template-id:rule-id>

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDiameterCapmGenericMinorAlarmNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

25007 - CAPM Generic Alarm - Major

Event Type:
CAPM

Description:
CAPM Generic Alarm - Major

Severity:
Major

Instance:
<template-id:rule-id>

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDiameterCapmGenericMajorAlarmNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

25008 - CAPM Generic Alarm - Critical

Event Type:
CAPM

Description:
CAPM Generic Alarm - Critical

Severity:
Critical

Instance:
<template-id:rule-id>

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDiameterCapmGenericCriticalAlarmNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

OAM Alarm Management (25500-25899)

This section provides information and recovery procedures related for alarms and events related to OAM Alarm Management, ranging from 25500 - 25899, that can occur on the system. All events have a severity of Info.

Alarms and events are recorded in a database log table. Currently active alarms can be viewed from the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the Alarms & Events > View History page.

25500 - No DA-MP Leader Detected Alarm

Alarm Group:
DIAM

Description:
This alarm occurs when no active DA-MP leaders have been detected.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterNoDaMpLeaderDetectedNotify

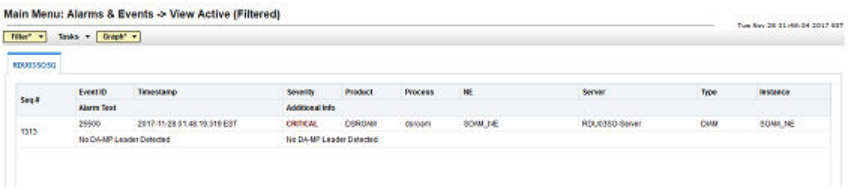
Cause:
The alarm # 25500 raises:

- When No Active DA-MP leaders are reported by the maintenance leader.
- When there is a single DA-MP and DSR process is stopped.
- When there are multiple DA-MPs, DSR process is stopped and there is ComAgent Connection failure between two or more DA-MP's.

The alarm clears when maintenance leader reports a single active DA-MP leader.

Diagnostic Information:

1. Examine the alarm log from **Main Menu > Alarms & Events** on Active SOAM Server.



2. This alarm is raised against the Network Element when no DA-MPs report themselves as **Leader**.

1. Recovery:

1. Verify the MP operational status of the DA-MP from the **Diameter**, and then **Maintenance**, and then **DA-MP** active SOAM screen.
   a. Verify the # Peer MPs Unavailable column displays 0 for each DA-MP server.
   b. Verify all DA-MP servers are available in individual DA-MP server tabs on the **Diameter**, and then **Maintenance**, and then **DA-MP** active SOAM screen.
   c. Verify ComAgent inter-MP connections (auto) are in the InService state on the **Communication Agent**, and then **Maintenance**, and then **Connection Status** screen.

2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25510 - Multiple DA-MP Leader Detected Alarm

Alarm Group:
DIAM

Description:
This alarm occurs when multiple active DA-MP leaders have been detected.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMultipleDaMpLeadersDetectedNotify

Cause:
The alarm #25510 raises:

- When more than one DA-MP report themselves as **Leader**.
- When DSR process is running on all DA-MPs and ComAgent Connection is down between two or more DA-MP's.

The alarm clears when maintenance leader reports a single active DA-MP leader.

Diagnostic Information:

- This alarm is raised against the Network Element when multiple DA-MPs report themselves as **Leader**.
- Examine the alarm log from **Main Menu > Alarms & Events** on Active SOAM Server.
- When this alarm is raised Existing IPFE Connection, Route List, and Peer Node alarms will be cleared.
- New IPFE Connection, Route List, and Peer Node alarms are suppressed.

1. Recovery:

1. Verify the MP operational status of the DA-MP from the **Diameter**, and then **Maintenance**, and then **DA-MP** active SOAM screen.
    a. Verify the # Peer MPs Unavailable column displays 0 for each DA-MP server.
    b. Verify all DA-MP servers are available in individual DA-MP server tabs on the **Diameter**, and then **Maintenance**, and then **DA-MP** active SOAM screen.

c. Verify ComAgent inter-MP connections (auto) are in the InService state on the **Communication Agent**, and then **Maintenance**, and then **Connection Status** screen.

2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25800 - Peer Discovery Failure

Alarm Group:
DIAM

Description:
Peer discovery failure.

Severity:
Minor

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has failed.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDpdRealmDiscoveryFailedNotify

1. Recovery:
1. Analyze event 25801 - Peer Discovery Configuration Error Encountered that has the same instance to identify the error(s).
2. Verify the DSR and DNS configurations and fix any configuration error(s).
3. Administratively refresh the Realm.
4. It is recommended to contact My Oracle Support for assistance.

25801 - Peer Discovery Configuration Error Encountered

Event Type:
DIAM

Description:
Peer discovery configuration error encountered.

Severity:
Info

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has encountered a configuration error.

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDpdConfigErrorNotify

1. Recovery:
1. Depending on the specific error code, follow the appropriate recovery steps.

> **Note:**
>
> One likely cause is the number of instances of a managed object type is at capacity, and no new instances can be created. The user can delete unused instances of the MO type to free up capacity and try the Realm discovery again.

2. It is recommended to contact My Oracle Support for assistance.

25802 - Realm Expiration Approaching

Alarm Group:
DIAM

Description:
Realm expiration approaching.

Severity:
Minor, Major

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose expiry is approaching.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDpdConfigErrorNotify

1. Recovery:
1. Administratively disable the Realm.
2. Administratively extend the Realm.
3. Administratively refresh the Realm.
4. It is recommended to contact My Oracle Support for assistance.

25803 - Peer Discovery - Inconsistent Remote Host Port Assignment

Event Type:
DIAM

Description:
Peer discovery - inconsistent remote host port assignment.

Severity:
Info

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery has encountered inconsistent remote host port assignment.

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDpdInconsistentPortAssignmentNotify

1. Recovery:

- No action required. The DNS records for the Realm being discovered must be corrected by the Realm's DNS administrator.

25804 - Peer Discovery State Change

Event Type:
DIAM

Description:
Peer discovery state change.

Severity:
Info

Instance:
Discover_Realm_{realm_name} where {realm_name} is the full configured name of the Realm whose discovery state has changed.

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDpdInconsistentPortAssignmentNotify

1. Recovery:

- No action required.

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

1. Recovery:

- 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

1. Recovery:

- 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

1. 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 - 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

Cause:
This alarm is caused by an application thread which fails to respond to the platform process management subsystem heartbeat within the defined time period. The actual cause may vary depending on the differing threads and defined time periods.

Diagnostic Information:
Collect the following data before contacting My Oracle Support for assistance.

- iqt -Ep PmControl on the issuing server.
- Savelogs_Plat on the issuing server.
- Alarm history from active SOAM server.

1. Recovery:

1. Alarm indicates an application failed to respond to the platform process management subsystem heartbeat within the defined period. Export event history for the given process to narrow the actual cause.
2. If this problem persists, collect Savelogs and it is recommended to contact My Oracle Support.

31100 - Database replication fault

Alarm Group:
SW

Description:
The database replication process 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:
eagleXgDsrDbRepToSlaveFailureNotify

1. Recovery:

1. Export event history for the affected 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:
Critical

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepToSlaveFailureNotify

Cause:
Alarm 31101 raises 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 could not get the slave's correct HA state as 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.

Diagnostic Information:

1. Verify the path for all services on a node:
   a. In a command interface, type `path.test -a <toNode>` to test the paths for all services.

2. In a command interface, use the path test commands to test the communication between nodes:
   a. Run the command, `iqt -pE NodeInfo` to get the node ID
   b. Then, run the command, `path.test -a <nodeid>` to test the paths for all services
3. Examine the Platform savelogs on all MPs, SO, and NO:
   a. Run the command, **sudo /usr/TKLC/plat/sbin/savelogs_plat**
   b. The plat savelogs in the **/tmp** directory.

1. 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 `iqt -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

Cause:
Alarm 31102 raises when the replication slave finds the replication link is disconnected from the master.

Diagnostic Information

1. Verify the path for all services on a node:
   a. In a command interface, run the command, `path.test -a <toNode>` to test the paths for all services.
2. In a command interface, use the path test command to test the communication:
   a. Run the command, `iqt -pE NodeInfo` to get the node ID
   b. Run the command, `path.test -a <nodeid>` to test the communication path
3. Examine the Platform savelogs on all MPs, SO, and NO:
   a. Run the command, `sudo /usr/TKLC/plat/sbin/savelogs_plat`
   b. The plat savelogs are in the **/tmp**directory.

1. 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 `iqt -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 database.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepUpdateFaultNotify

1. 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:
eagleXgDsrDbRepLatencyNotify

1. 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

1. 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

Cause:
DB merging to the Parent Merge Node has failed.

Diagnostic Information:

- Check if the states are either **Active** or **Standby** (for example, none are DownConnecting or Auditing).
- Check if there are issues with merging or replication or with communication. Can the primary active NO talk to the server with the issue and visa versa. run the command `path.test` command.

> **Note:**
>
> If checking information for an MP server, also check it's SOAM server that it would merge to or receive replicated data from:

- `soapstat -w`
- `irepstat -w`
- `inetmstat -w`
- `path.test -a -r`

> **Note:**
>
> In older releases, the '-r' option is not available.

- **cat /var/tmp/dbreinitstate**

1. 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:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeFromChildFailureNotify

1. 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

1. 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

1. 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

1. 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

1. Recovery:

- 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

1. 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

1. Recovery:

- 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

1. 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

1. 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:
eagleXgDsrExcessiveSharedMemoryConsumptionNotify

1. Recovery:

- This alarm indicates a server has exceeded the engineered limit for shared memory usage and there is a risk the 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:
eagleXgDsrLowDiskFreeNotify

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. Recovery:

- 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

1. Recovery:

- 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:
eagleXgDsrDbDurabilityDegradedNotify

1. 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:
eagleXgDsrAuditBlockedNotify

1. Recovery:

- This alarm indicates the 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

1. Recovery:

- 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:
eagleXgDsrDbADICErrorNotify

1. 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

1. Recovery:

- 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

1. 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

1. Recovery:

1. This alarm indicates 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 `procshm -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

1. Recovery

- 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
eagleXgDsrDbRepSwitchoverNotify

1. 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

1. 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

1. 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

1. Recovery

- 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
eagleXgDsrDbSiteRepLatencyNotify

1. 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

1. 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

1. 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:
eagleXgDsrDbMastershipFaultNotify

1. 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

1. 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

1. 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.

31149 - DB late write nonactive

Alarm Group
DB

Description
Application wrote to database while HA role change from active was in progress.

Severity
Minor

Instance
HA resource name

HA Score
Normal

Auto Clear Seconds
3600

OID
comcolDbLateWriteNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance.

31150 - DB Health Impacted

Alarm Group:
DB

Description:
Database health impacted

Severity:
Critical

Instance:
xxx

HA Score:
xxx

Auto Clear Seconds:
##

OID:
xxx

1. Recovery:

- If the problem persists, it is recommended to contact My Oracle Support.

31151 – DB Storage Persistent Failure

Alarm Group
DB

Description
Persistent database failure

Severity
Critical

Instance:
xxx

HA Score:
xxx

Auto Clear Seconds:
##

OID:
xxx

1. Recovery:

- If the problem persists, 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

1. 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:
Critical

Instance:
May include process name

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDsrProcNotRunningNotify

Cause:
Internal error occurs and application shut down abruptly. A managed process cannot be started or has been terminated unexpectedly .

Diagnostic Information:

1. If this alarm is observed during installation of DSR system, and alarm instance is EXGSTACK_Process, make sure the DAMP Profile Assignment procedure is complete on the active SOAM for all DA-MPs.
2. During application start and shutdown, a temporary error may result while restarting the application.
   a. The alarm automatically clears in 300 seconds if it was caused by a temporary error that no longer exists now.
   b. The alarm exists, if the error is not recovered.
3. If alarm is raised after any unapproved configuration change, try to revert back the configuration and check if alarm clears.

> **Note:**
>
> In a few cases, the alarm may stay for more than 300 seconds even if error condition is corrected. In such cases, wait for 300 seconds after corrective actions, before reporting it.

1. Recovery:

1. This alarm indicates a managed process cannot be started and has unexpectedly terminated.
2. It is recommended to contact My Oracle Support.

31202 - Unkillable zombie process

Alarm Group:
PROC

Description:
A zombie process exists that cannot be killed by procmgr. procmgr no longer manages this process.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDsrProcZombieProcessNotify

1. Recovery:

1. This alarm indicates a 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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:
eagleXgDsrHaHbTransmitFailureNotify

1. 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:
eagleXgDsrHaCfgErrorNotify

1. 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:
Critical

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0

OID:
eagleXgDsrHaSvcStartFailureNotify

Cause:
The COMCOL module reports the 31225 alarm when the required HA resource fail to start.

Diagnostic Information:
On the active NO, get the content of the following these tables by executing the commands:

- `iqt -E HaClusterPolicyCfg`
- `iqt -E HaClusterResourceCfg`
- `iqt -E HaNodeLocPref`
- `iqt -E HaResourceCfg`
- `ha.info` on active NO, SO and all MPs

1. Recovery:

1. This alarm clears automatically when the HA daemon successfully starts.
2. If this alarm does not clear after a couple minutes, collect logs in Diagnostic information and 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:
eagleXgDsrHaAvailDegradedNotify

1. 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:
eagleXgDsrHaAvailFailedNotify

Cause:
This alarm raises when there are alarms with haScore="FAILED", and displayed in the GUI.

Diagnostic Information:

- Get the `iqt -E RecentAlarmEv.1` result on active SO server.
- Get Savelogs on active SO server.
- Get `err.show` output on active SO server.

1. 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, collect logs in Diagnostic information and 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:
eagleXgDsrHaStandbyOfflineNotify

Cause:
There are HA heartbeat messages among the servers. If the servers, such as NO and SO, cannot get the HA heartbeat from its mate even after trying several times, the alarm raises. The default interval time is 250 ms. The alarm raises after retrying five times.

Diagnostic Information:
To diagnose the alarm further, perform the following:

- The platform savelogs on active NO and SO servers.
- Get **iqt -E HaCfg** from active NO and SO servers.

1. Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, the 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 it is recommended to contact My Oracle Support, if needed.
3. A workaround for this problem is to increase the failCount values for all server groups in the HaCfg table. Bumping it from 5 to 10 should solve the problem. Check with the application team before applying this workaround. Run the `iset -ffailCount=10 HaCfg` command on the active NO where "1=1".

> **Note:**
>
> This command is disruptive and causes active servers in the entire topology to lose service for about one minute while HA is reconfigured. A new server may be selected as active after the change is applied. If less disruption is required, you can apply the change one server group at a time as an alternative.

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

1. Recovery:

- 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

1. 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

1. 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

1. Recovery:

- 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:
eagleXgDsrHaPathDownNotify

1. 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 often requires rebooting the server.

Severity:
Critical

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrUtrustedTimeOnInitNotify

Cause:

- NTP is misconfigured
- NTP servers are unreachable
- NTP service not running

Diagnostic Information:
There are often accompanying Platform alarms to guide correction. Applications do not start if time is not accurate on start-up. Recovery often requires rebooting the server.

1. 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, or the NTP service (ntpd process) has stopped. There are often accompanying Platform alarms to guide correction. Generally, applications remain running, but time-stamped data are likely incorrect, reports may be negatively affected, or some behavior may be improper.

Severity:
Critical

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrUtrustedTimePostInitNotify

Cause:

- NTP has reconfigured improperly after system initialization
- System time has been manually changed
- The NTP servers have become unreachable
- NTP service (ntpd process) stopped

Diagnostic Information:
There are often accompanying Platform alarms to guide correction.

1. 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:
eagleXgDsrHaLinkDownNotify

1. 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

1. 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 software fault.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolRePortMappingFaultNotify

1. Recovery:

- 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 software fault.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDsrDbcomcolSnmpAgentNotify

1. 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

1. 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

1. Recovery:

- 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

1. 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

1. 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

1. 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:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrHaServerOfflineNotify

Cause:
The 31283 alarm presents for nodes in the topology that you should be connected to (for example, 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 (for example, networking connectivity, and node not running, etc.).

Diagnostic Information:
Show the alarms that affect the node's HA score:

```
iqt -h -fpart,no -fsrcNode,no -fsrcTimeStamp,no -p
AppEventLog.0 where "eventNumber in (`iqt -S, -zhp -fnumber
AppEventDef where "haScore != 0" | sed -e's/,$//'`)"
```

1. Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, the 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

1. 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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
eagleXgDsrHaBadSiteCfgNotify

1. Recovery

- 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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 (for example, 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

1. 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- This event is used for internal logging. No action is required.

31297 - HA resource agent info

Alarm Group:
HA

Description:
HA resource agent information.

Severity:
Info

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaInfoNotify

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery

- It is recommended to contact My Oracle Support.

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

1. Recovery:

- 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

1. Recovery

- 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:
tpdBrkPnlMntFailure

1. Recovery

- It is recommended to 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

1. Recovery

- 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

1. Recovery

- 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

1. Recovery

- 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:
tpdPowerSupply3Failure

1. Recovery

- It is recommended to 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:
eagleXgDsrTpdRaidFeedUnavailableNotify

1. Recovery

- 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

1. Recovery

- 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

1. Recovery

- 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

1. Recovery

- 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:
eagleXgDsrTpdDeviceFailureNotify

1. Recovery:

- It is recommended to contact My Oracle Support to request hardware replacement.

32112 - Device interface failure

Alarm Group:
PLAT

Description:
This alarm indicates either the IP bond is not configured or is down.

Severity:
Critical

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrTpdDeviceIfFailureNotify

Cause:
This alarm indicates either the IP bond is not configured or down.

Diagnostic Information:

- Syscheck can be manually executed in the following methods:
  - Login as syscheck. When logging in, syscheck runs and then the login connection is dropped. This account does not have shell access.
  - From the root accoun,t the Command Line Interface can be utilized directly.
    * Execute `syscheck -h` for usage information.
  - In DSR 6.0 and later, from the admusr account the Command Line Interface can be used directly when called using `sudo`.
    * Execute `syscheck -h` for usage information.
  - Using the platcfg user interface.

> **Note:**
>
> In versions later than TPD 6.5, root access using SSH is disabled. The admusr should be used instead. If the command is to be run as admusr, sudo must be prepended to the command and the full path to the command must be used.

- `sudo /usr/TKLC/plat/bin/netAdm query --device=<bondX>`
- `sudo /usr/TKLC/plat/bin/netAdm query --device=<slave device>`
- `cat /proc/net/bonding/bondX`, where X is bond designation
- ethtool <slave device>

1. Recovery:

1. Run `syscheck` in verbose mode by executing `syscheck -h` for usage information.
2. Investigate the failed bond and slave devices configuration using `netAdm` query:
   - `sudo /usr/TKLC/plat/bin/netAdm query --device=<bondX>`
   - `sudo /usr/TKLC/plat/bin/netAdm query --device=<slave device>`
3. Determine if the failed bond and slave devices have been administratively shut down or have operational issues:
   - `cat /proc/net/bonding/bondX`, where X is bond designation
   - `ethtool <slave device>`

4. If bond and slaves are healthy, attempt to administratively bring bond up:
   - `ifup bondX`
5. If condition persists, contact My Oracle Support and provide the system health check output and output of steps 1 through 4.
6. It is recommended to contact My Oracle Support to request hardware replacement.

32113 - Uncorrectable ECC memory error

Alarm Group:
PLAT

Description:
This alarm indicates the chipset has detected an uncorrectable (multiple-bit) memory error 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:
eagleXgDsrTpdEccUncorrectableErrorNotify

Alarm ID:
TKSPLATCR14

Cause:
This alarm indicates chipset has detected an uncorrectable (multiple-bit) memory error the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Diagnostic Information:
Syscheck can be manually executed using the following methods:

- Login as syscheck. When logging in, syscheck runs and the login connection is dropped. This account does not have shell access.
- From the root account the Command Line Interface can be used directly.
  - Execute `syscheck -h` for usage information.
- In DSR 6.0 and later, from the admusr account the Command Line Interface can be used directly when called using `sudo`.
  - Execute `syscheck -h` for usage information.
- Through the platcfg user interface.

> **Note:**
>
> In versions later than TPD 6.5, root access using SSH is disabled. The admusr should be used instead. If the command needs to be run as admusr, sudo must be prepended to the command and the full path to the command must be used.

1. Recovery:

- It is recommended to contact My Oracle Support 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:
eagleXgDsrTpdSNMPGetFailureNotify

Alarm ID:
TKSPLATCR15

Cause:
This alarm indicates the server failed to get SNMP information from the device configured in the SNMPGET syscheck test.

Diagnostic Information:
Syscheck can be manually executed using the following methods:

- Login as syscheck. When logging in, syscheck runs and the login connection is dropped. This account does not have shell access.
- From the root account the Command Line Interface can be used directly.
  - Execute `syscheck -h` for usage information.

- In DSR 6.0 and later, from the admusr account the Command Line Interface can be used directly when called using sudo.
  - Execute `syscheck -h` for usage information.
- Using the platcfg user interface.

> **Note:**
>
> In versions later than TPD 6.5, root access using SSH is disabled. The admusr should be used instead. If the command needs to be run as admusr, sudo must be prepended to the command and the full path to the command must be used.

1. Recovery:

1. Verify the 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 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:
eagleXgDsrTpdNTPDaemonNotSynchronizedFailureNotify

Alarm ID:
TKSPLATCR16

Cause:
The server's current time precedes the timestamp of the last known time when the server's time was good.

Diagnostic Information:
N/A.

1. 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 -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 of 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.

   - Reset ntpd:
   - `sudo service ntpd stop`
   - `sudo ntpdate <ntp server IP>`
   - `sudo service ntpd start`
4. Confirm 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 on a virtualized server.
   - Additional recommendations and topology are available in the 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 servers time was good.

Severity:
Critical

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrTpdNTPTimeGoneBackwardsNotify

Alarm ID:
TKSPLATCR17

Cause:
The server's current time precedes the timestamp of the last known time when the servers time was good.

Diagnostic Information:
N/A.

1. 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 of 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.

- Reset ntpd:
- `sudo service ntpd stop`
- `sudo ntpdate <ntp server IP>`
- `sudo service ntpd start`

4. Confirm 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 the 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 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:
eagleXgDsrNtpOffsetCheckFailureNotify

Alarm ID:
TKSPLATCR18

Cause:
The NTP offset of the server currently being synced to is greater than the critical threshold.

Diagnostic Information:
Run `ntpstat` command to diagnose the alarm.

1. 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 the peer can be reached.

2. If ntp peer is reachable, then restart the ntpd service.

3. If problem persists, then a reset of 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.

- To reset date:
- `sudo service ntpd stop`
- `sudo ntpdate <ntp server IP>`
- `sudo service ntpd start`

4. Confirm 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 the 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 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:
eagleXgDsrTpdFanErrorNotify

Alarm ID:
TKSPLATMA1

1. 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:
eagleXgDsrTpdIntDiskErrorNotify

Alarm ID:
TKSPLATMA2

1. 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 the off-board 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:
eagleXgDsrTpdRaidDiskErrorNotify

Alarm ID:
TKSPLATMA3

1. Recovery

1. Determine if the hardware platform is PP5160.

   > **Note:**
   >
   > SDM on the PP5160 platform uses raid0 configuration.

   If the platform is a PP5160, no action is required.
2. 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:
eagleXgDsrTpdPlatformErrorNotify

Alarm ID:
TKSPLATMA4

1. 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.

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:
eagleXgDsrTpdFileSystemErrorNotify

Alarm ID:
TKSPLATMA5

1. 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 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:
eagleXgDsrTpdPlatProcessErrorNotify

Alarm ID:
TKSPLATMA6

1. 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:
eagleXgDsrTpdRamShortageErrorNotify

1. Recovery

- It is recommended to contact My Oracle Support.

32307 - Server swap space shortage failure

Alarm Group:
PLAT

Description:
This alarm indicates 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:
eagleXgDsrTpdSwapSpaceShortageErrorNotify

Alarm ID:
TKSPLATMA8

1. 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 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:
eagleXgDsrTpdProvNetworkErrorNotify

Alarm ID:
TKSPLATMA9

1. 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 the chipset has detected an uncorrectable (multiple-bit) memory error 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:
eagleXgDsrTpdEagleNetworkAErrorNotify

1. Recovery

- 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 the chipset has detected an uncorrectable (multiple-bit) memory error 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:
eagleXgDsrTpdEagleNetworkBErrorNotify

1. Recovery

- 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 the chipset has detected an uncorrectable (multiple-bit) memory error 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:
eagleXgDsrTpdSyncNetworkErrorNotify

1. Recovery

- 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 one of these 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:
eagleXgDsrTpdDiskSpaceShortageErrorNotify

Alarm ID:
TKSPLATMA13

1. 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 the default network route of the server is experiencing a problem.

> **Caution:**
>
> When changing the network routing configuration of the server, verify 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:
eagleXgDsrTpdDefaultRouteNetworkErrorNotify

1. 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 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

1. Recovery:

1. Ensure nothing is blocking the fan intake. Remove any blockage.
2. Verify 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 one or more of the monitored voltages on the server main board 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

1. 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 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:
eagleXgDsrTpdPowerFeedErrorNotify

Alarm ID:
TKSPLATMA17

1. Recovery:

1. Verify 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:
eagleXgDsrTpdDiskHealthErrorNotify

Alarm ID:
TKSPLATMA18

1. 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:
eagleXgDsrTpdDiskUnavailableErrorNotify

Alarm ID:
TKSPLATMA19

1. 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 the off-board storage server had a problem with its disk volume filling up.

Severity:
Major

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrTpdDeviceErrorNotify

Alarm ID:
TKSPLATMA20

1. Recovery

- It is recommended to contact the My Oracle Support.

32320 - Device interface error

Alarm Group:
PLAT

Description:
This alarm indicates 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:
eagleXgDsrTpdDeviceIfErrorNotify

Alarm ID:
TKSPLATMA21

1. 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/bond`X, 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

1. 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 the 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

1. Recovery:

1. Verify nothing is obstructing the airflow to the fans of the power supply.
2. Run syscheck in verbose mode. The output provides 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) probably needs to be replaced.

32323 - Power supply B error

Alarm Group:
PLAT

Description:
This alarm indicates the 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

1. Recovery:

1. Verify nothing is obstructing the airflow to the fans of the power supply.

2. Run syscheck in verbose mode. The output provides 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) probably needs to be replaced.

32324 - Breaker panel feed error

Alarm Group:
PLAT

Description:
This alarm indicates 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:
eagleXgDsrTpdBrkPnlFeedErrorNotify

Alarm ID:
TKSPLATMA25

1. Recovery:
1. Verify 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 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

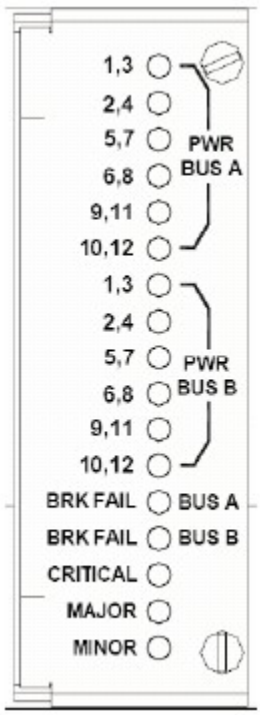
Description:
This alarm indicates a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see Figure 3-1) identify whether the fault occurred on the input power or the output power, as follows:

- 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 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 the output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B is 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)

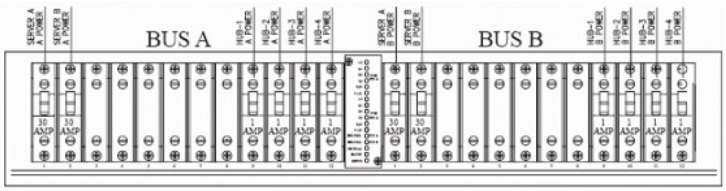
OID:
eagleXgDsrTpdBrkPnlBreakerErrorNotify

Alarm ID:
TKSPLATMA26

1. Recovery:

1. Verify 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 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 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 these steps to correct this problem:

- Verify 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 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:**
>
> Make 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; proceed to step 4 to verify 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 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 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 the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel are 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:
eagleXgDsrTpdBrkPnlMntErrorNotify

Alarm ID:
TKSPLATMA27

1. Recovery:

1. Verify 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 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 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 the 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:
eagleXgDsrTpdHaKeepaliveErrorNotify

Alarm ID:
TKSPLATMA28

1. 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 heartbeart 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 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:
eagleXgDsrTpdDrbdUnavailableNotify

Alarm ID:
TKSPLATMA29

1. Recovery

- It is recommended to contact My Oracle Support.

32329 - DRBD is not replicating

Alarm Group:
PLAT

Description:
This alarm indicates DRBD is not replicating to the peer server. Usually this indicates 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:
eagleXgDsrTpdDrbdNotReplicatingNotify

Alarm ID:
TKSPLATMA30

1. Recovery

- It is recommended to contact My Oracle Support.

32330 - DRBD peer problem

Alarm Group:
PLAT

Description:
This alarm indicates 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:
eagleXgDsrTpdDrbdPeerProblemNotify

Alarm ID:
TKSPLATMA31

1. Recovery

- It is recommended to contact the My Oracle Support.

32331 - HP disk problem

Alarm Group:
PLAT

Description:
This major alarm indicates there is an issue with either a physical or logical disk in the HP disk subsystem. The message includes 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:
eagleXgDsrTpdHpDiskProblemNotify

Alarm ID:
TKSPLATMA32

1. 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 does not since there is no battery.
3. If Cache Status is Permanently Disabled and Cache Status Details indicated the cache is disabled and 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 there is an issue with an HP disk controller. The message includes 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:
eagleXgDsrTpdHpDiskCtrlrProblemNotify

Alarm ID:
TKSPLATMA33

1. 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 there is an issue with the process that caches the HP disk subsystem status. This usually means 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:
eagleXgDsrTpdHPACUCLIProblemNotify

Alarm ID:
TKSPLATMA34

1. 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 it was not administratively stopped.

> **Note:**
>
> The disk status daemon is named either TKLChpacucli or TPDhpDiskStatus in more recent versions of TPD.

   - Executing `status TPDhpDiskStatus`, or `status TKLChpacucli` depending on TPD release, should produce output indicating the process is running.
4. If not running, attempt to start the HP disk status process with `start TPDhpDiskStatus`, or if appropriate `start TKLChpacucli` .

5. Verify there are no hpssacli or hpacucli error messages in /var/log/messages. If there are this could indicate the HP utility is hung. If the HP hpssacli utility or hpacucli utility is hung, proceed to the 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:
eagleXgDsrTpdMpathDeviceProblemNotify

1. Recovery:

- 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:
eagleXgDsrTpdSwitchLinkDownErrorNotify

Alarm ID:
TKSPLATMA36

1. 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 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:
eagleXgDsrTpdHalfOpenSockLimitNotify

Alarm ID:
TKSPLATMA37

1. 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 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:
eagleXgDsrTpdFlashProgramFailureNotify

Alarm ID:
TKSPLATMA38

1. Recovery:

- It is recommended to contact My Oracle Support.

32338 - Serial mezzanine unseated

Alarm Group:
PLAT

Description:
This alarm indicates 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:
eagleXgDsrTpdSerialMezzUnseatedNotify

Alarm ID:
TKSPLATMA39

1. Recovery:

1. Ensure 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 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:
eagleXgDsrTpdMaxPidLimitNotify

Alarm ID:
TKSPLATMA40

1. 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 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:
eagleXgDsrTpdNTPDaemonNotSynchronizedErrorNotify

Alarm ID:
TKSPLATMA41

1. Recovery:
1. Verify NTP settings and 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 resetting 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.

   - 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 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:
eagleXgDsrTpdNTPDaemonNeverSynchronizedNotify

Alarm ID:
TKSPLATMA42

1. 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 resetting 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.

- 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:
eagleXgDsrNtpOffsetCheckErrorNotify

Alarm ID:
TKSPLATMA43

1. 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 resetting 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.

- 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 the 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:
eagleXgDsrTpdDiskProblemNotify

Alarm ID:
TKSPLATMA44

1. 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 the RAID controller needs intervention.

Severity:
Major

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrTpdDiskCtrlrProblemNotify

Alarm ID:
TKSPLATMA45

1. 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 the 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:
eagleXgDsrTpdUpgradeSnapshotInvalidNotify

Alarm ID:
TKSPLATMA46

1. 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 the 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

1. 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:
eagleXgDsrTpdHWMGMTCLIProblemNotify

Alarm ID:
TKSPLATMA47

1. 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 hwmgmtd process is running. If not running, verify it was not administratively stopped.
   - Execute `service hwmgmtd status` to produce output indicating the process is running.
   - If not running, attempt to start process `service hwmgmtd status`.
4. Determine if the TKLChwmgmtcli process is running. If not running, verify it was not administratively stopped.
   - Execute `status TKLChwmgmtcli` to produce output indicating the process is running.
   - If not running, attempt to start process `start TKLChwmgmtcli`.
5. Verify there are no hwmgmt error messages in /var/log/messages. If there are this could indicate the Oracle utility is hung. If hwmgmtd 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:
eagleXgDsrTpdFipsSubsystemProblemNotify

1. 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:
eagleXgDsrTpdHidsFileTamperingNotify

1. Recovery:

- It is recommended to contact My Oracle Support.

32350 - Security process terminated

Alarm Group:
PLAT

Description:
This alarm indicates 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:
eagleXgDsrTpdSecurityProcessDownNotify

1. Recovery:

- 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

1. 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

1. 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 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

1. 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

1. Recovery

1. Refer to MPS-specific documentation for information regarding this alarm.
2. It is recommended to contact 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

1. Recovery

- It is recommended to contact My Oracle Support.

32505 - Server swap space shortage warning

Alarm Group:
PLAT

Description:
This alarm indicates 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

1. Recovery:

1. Run syscheck in verbose mode.
2. Determine which processes are using swap.
   a. List application processes and determine the process ID.
   b. Determine how much swap each process is using. 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, provide the system health check output, and process swap usage.

32506 - Server default router not defined

Alarm Group:
PLAT

Description:
This alarm indicates the default network route is either not configured or the current configuration contains an invalid IP address or hostname.

> **Caution:**
>
> When changing the server's network routing configuration, it is important to verify the modifications do not impact the method of connectivity for the current login session. It is also crucial this information not be entered incorrectly or set to improper values. Incorrectly modifying the server's routing configuration may result in total loss of remote network access.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDefaultRouteNotDefined

Alarm ID:
TKSPLATMI7

1. 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 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 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 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

1. Recovery:

1. Ensure nothing is blocking the fan intake. Remove any blockage.
2. Verify 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 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 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

1. Recovery:
1. It is recommended to contact My Oracle Support to create a service request.
2. On the affected server, execute 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 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:
tpdNTPDeamonNotSynchronizedWarning

Alarm ID:
TKSPLATMI10

1. 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 resetting 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.

- 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 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 causes problems if 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

1. Recovery:

- 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

1. 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

1. 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

1. 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 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

1. Recovery:

- It is recommended to contact My Oracle Support.

32515 - Server HA failover inhibited

Alarm Group:
PLAT

Description:
This alarm indicates 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

1. Recovery:

- It is recommended to contact My Oracle Support.

32516 - Server HA active to standby transition

Alarm Group:
PLAT

Description:
This alarm indicates 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

1. Recovery:

- It is recommended to contact My Oracle Support.

32517 - Server HA standby to active transition

Alarm Group:
PLAT

Description:
This alarm indicates 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

1. Recovery:

- 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

1. Recovery:

- It is recommended to contact My Oracle Support.

32519 - NTP offset check failure

Alarm Group:
PLAT

Description:
This minor alarm indicates the 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

1. 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 resetting 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.

   - 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 NTP is synchronizing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The alarm message provides the stratum value of the NTP server and the stratum limit 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

1. 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 resetting 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.

   - 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 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

1. Recovery:

- It is recommended to contact My Oracle Support to get a replacement sensor.

32522 - SAS drive missing

Alarm Group:
PLAT

Description:
This alarm indicates 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

- It is recommended to contact My Oracle Support.

32523 - DRBD failover busy

Alarm Group:
PLAT

Description:
This alarm indicates a DRBD synchronization 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 its 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

1. Recovery

- A DRBD synchronization 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, 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

1. 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 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

1. Recovery:

- 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 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

1. 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 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

1. 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 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

1. Recovery:

- 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 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

1. 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 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

1. Recovery:

- It is recommended to contact My Oracle Support.

32531 - Half open socket warning limit

Alarm Group:
PLAT

Description
This alarm indicates 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

1. 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 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

1. Recovery:

- 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 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

1. 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 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

1. 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 resetting 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.

- 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 the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message includes 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 75 minutes).

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskResync

Alarm ID:
TKSPLATMI36

1. 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 the upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots 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

1. 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 the FIPS subsystem requires a reboot to complete configuration.

Severity:
Minor

Instance:
May include AlarmLocation, AlarmId, AlarmState, AlarmSeverity, and bindVarNamesValueStr

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFipsSubsystemWarning

1. Recovery

- 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

1. Recovery
1. Run `/usr/TKLC/plat/bin/pdcAdm`. If run 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

1. Recovery

- 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- 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

1. Recovery:

- It is recommended to contact My Oracle Support.

32703 - HIDS enabled

Alarm Group:
PLAT

Description:
HIDS was enabled.

Default Severity:
Info

OID:
tpdHidsEnabled

1. Recovery:

- It is recommended to contact My Oracle Support.

32704 - HIDS disabled

Alarm Group:
PLAT

Description:
HIDS was disabled.

Default Severity:
Info

OID:
tpdHidsDisabled

1. Recovery:

- It is recommended to contact My Oracle Support.

32705 - HIDS monitoring suspended

Alarm Group:
PLAT

Description:
HIDS monitoring suspended.

Default Severity:
Info

OID:
tpdHidsSuspended

1. Recovery:

- It is recommended to contact My Oracle Support.

32706 - HIDS monitoring resumed

Alarm Group:
PLAT

Description:
HIDS monitoring resumed.

Default Severity:
Info

OID:
tpdHidsResumed

1. Recovery:

- It is recommended to contact My Oracle Support.

32707 - HIDS baseline updated

Alarm Group:
PLAT

Description:
HIDS baseline updated.

Default Severity:
Info

OID:
tpdHidsBaselineUpdated

1. Recovery:

- It is recommended to contact My Oracle Support.

Diameter Custom Applications (DCA) Framework Alarms and Events (33300-33630)

This section provides information and recovery procedures for differentiated DCA Framework alarms.

33300 - Create Application Version Failure

Event Type
DCA

Description
Dsroam failed to create application version on DcaLifecycleSoam table.

Severity
Info

Instance
DcaLifecycleNoam.verId

HA Score
Normal

Throttle Seconds
60

OID
dcaDcaCreateAppVersionFailureNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance.

33301 - Update Config Data Failure

Event Type
DCA

Description
Dsroam failed to synchronize configuration data on SO.

Severity
Info

Instance
ApplicationId.name

HA Score
Normal

Throttle Seconds
60

OID
dcaDcaUpdateConfigDataFailureNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance.

33302 - Delete Application Version Failure

Event Type
DCA

Description
Dsroam failed to delete application version from DcaLifecycleSoam table.

Severity
Info

Instance
DcaLifecycleSoam.verId

HA Score
Normal

Throttle Seconds
60

OID
dcaDcaDeleteAppVersionFailureNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance.

33303 - UDR Event Queue Utilization

Alarm Group
DCA

Description
The DSR Application UDR Event Queue Utilization is approaching its maximum capacity.

Severity
Minor, Major, Critical

Instance
RxDcaUdrEventMsgQueue [<*DcaDalId.dalId*>], DCA

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
dcaDSRAppUdrEventMessageQueueUtilizationNotify

1. Recovery
1. The DSR Application's UDR Result Message Queue is approaching its maximum capacity. This alarm typically does not occur when no other congestion alarms are asserted. The alarm may occur for a variety of reasons:

   The processing of the UDR results by the DCA application indicates the DCA application is overly CPU intensive. The alarm may also be the result of the DCA application sending too many UDR queries per Diameter message, which may be avoided by storing variables in the Diameter transaction context. In both cases, review and optimize the business logic.
2. If no additional congestion alarms are asserted, the DSR application Task may be experiencing a problem preventing it from processing messages from its UDR Event Message Queue. Examine the alarm log from **Alarms & Events**.
3. It is recommended to contact My Oracle Support for assistance if needed.

33304 - DCA Runtime Errors

Alarm Group
DCA

Description
The script generated runtime errors.

Severity
Critical

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:" and thread pool (Request, Answer or SBR Event)

HA Score
Normal

Auto Clear Seconds
60

OID
dcaDSRAppRuntimeErrorNotify

1. Recovery

- The error message generated by the Perl interpreter is included in the alarm's additional info.

  Fix the error accordingly and recompile the Perl script, or replace the Trial/Production version (depending on whether the DA-MP is a Trial DA-MP or not) with another script version.

> **Note:**
>
> Because the compilation occurs in parallel while the previously compiled script is still running (and hence keeps raising the alarm), a successful compilation will not immediately clear the alarm. There will be an auto clear latency of 20 seconds that will clear the alarm.

33305 - DCA Procedure Not Found

Alarm Group
DCA

Description
The Perl interpreter attempts to invoke a non-existent procedure.

Severity
Critical

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:" and thread pool (Request, Answer or UDR Event)

HA Score
Normal

Auto Clear Seconds
60

OID
dcaDSRAppProcedureNotFoundNotify

1. Recovery

- The name of the missing procedure is include in the alarm's additional info.

  The procedure names involved are either the configured Diameter request and answer event handler names (**Main Menu**, and then **DCA Framework**, and then **<Application Name>**, and then **General Options** on the NOAM) or the callback names coded in the Perl script.

  Possible resolutions are:

  1. Fix the procedure names in the Perl script and re-compile the Perl script
  2. Fix the procedure names in the configuration
  3. Replace the Trial/Production version (depending on whether the DA-MP is a Trial DA-MP or not) with another script version.

  > **Note:**
  >
  > Because the compilation occurs in parallel while the previously compiled script is still running (and hence keeps raising the alarm,) a successful compilation will not immediately clear the alarm. There will be an auto clear latency of 20 seconds that will clear the alarm.

33307 - Diameter Message Routing Failure Due To Full DRL Queue

Event Type
DCA

Description
Diameter message routing failure due to full DRL queue. Diameter egress message could not be sent because the DRL queue is full.

Severity
Info

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Throttle Seconds
60

OID
dcaEgressMsgRouteFailureDueToDrlQueueExhaustedNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance.

33308 - DCA to UDR ComAgent Error

Event Type
DCA

Description
DCA failed to send query to UDR due to ComAgent Error.

Severity
Info

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Throttle Seconds
60

OID
dcaComAgentSendFailureNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance.

33309 - DCA Script Compilation Error

Alarm Group
DCA

Description
The script generates compilation errors.

Severity
Critical

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
dcaDSRAppCompileErrorNotify

1. Recovery

- The error message generated by the Perl interpreter is included in the alarm's additional info.

Fix the error accordingly and recompile the Perl script, or replace the Trial/ Production version (depending on whether the DA-MP is a Trial DA-MP or not) with another script version.

33311 - DCA Application Reloaded

Event Type
DCA

Description
The DCA application script has been successfully re-compiled and re-loaded.

Severity
Info

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Throttle Seconds
0 (zero)

OID
dcaDcaAppReloadedNotify

1. Recovery

- No action required.

33312 - DCA Script Generation Error

Alarm Group
DCA

Description
The script could not be saved in the `/tmp/appworks_temp` directory.

Severity
Critical

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
dcaDSRAppScriptGenerationErrorNotify

1. Recovery

- Ensure that enough space is available on the partition where `/tmp/appworks_temp` resides and re-initiate the script compilation.

33315 - DCA Asynchronous Task Stops Processing

Alarm Group:
DCA

Description:
DCA Asynchronous Task has stopped processing of Logging Events.

Severity:
Minor, Major

Instance:
The DCA App short name (DcaDalId.shortName) prefixed with "DCA:" and suffixed with DcaAsyncTaskId.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
DcaLoggingFailureNotify

Trigger Condition:
Low disk space or High event rate or file I/O error.

- It is recommended to contact My Oracle Support if further assistance is needed.

33316 - DCA AsyncTask Queue Utilization

Alarm Group:
DCA

Description:
The DSR application DCA AsyncTask queue utilization is approaching its maximum capacity.

Severity:
Minor , Major, Critical

Instance:
The DCA App short name (DcaDalId.shortName) prefixed with DCA:

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
DSRAppDcaAsyncMessageQueueUtilizationNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

33317 - DCA Fetch Log Error

Alarm Group:
DCA

Description:
DCA fetch log script has stopped working on the active SO.

Severity:
Minor

Instance:
The DCA App short name (DcaDalId.shortName) prefixed with DCA:

HA Score:
Normal

Auto Clear Seconds:
600

OID:
DcaFetchLogFailure

- It is recommended to contact My Oracle Support if further assistance is needed.

33318 - DCA CreateAndSend Request Message Send Failed

Alarm Group
DCA

Description
DCA failed while sending a CreateAndSend Request message.

Severity
Major

Instance
The DCA App short name (DcaDalId.shortName) prefixed with DCA:

HA Score
Normal

Auto Clear Seconds
600

OID
DCACreateAndSendRequestMessageSendFailed

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

DCA Custom MEAL Event Templates

33330-33429 - *DcaCustomMeal.name* + "Alrm"

Alarm Group
DCA

Description
DcaCustomMeal.descr

Severity
Minor, Major, Critical

Instance
"DCA:" concatenated with the *DcaDalId.shortName*

HA Score
Normal

Auto Clear Seconds
DcaCustomMeal.autoClearSecs (300 by default)

OID
"DcaCustomNotification" concatenated with the *DcaCustomMeal.id*

33430-33630 - DcaCustomMeal.name + "Alrm"

Alarm Group
DCA

Description
DcaCustomMeal.descr

Severity
Minor, Major, Critical

Instance
"DCA:" concatenated with the *DcaDalId.shortName*

HA Score
Normal

Auto Clear Seconds
DcaCustomMeal.autoClearSecs (300 by default)

OID
DcaCustomNotification concatenated with the *DcaCustomMeal.id*

Independent SBR Alarms and Events (12003-12010, 33730-33830)

12003 - SBR congestion state

Event Type:
SBRA

Description :
The SBR application is in a congested state and is shedding operations. The Sbr.RxIngressMsgQueueAvg measurement shows the average percentage of queue length utilization, which is used to determine congestion.

Severity:
Minor, Major, Critical

Instance:
Sbr.RxIngressMsgQueueMetric[subId], SBR

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
sbrCongestionState

Cause:
The SBR application is in a congested state due to high traffic load.

Diagnostic Information:
The SBR queue congestion alarm can have default onset and abatement thresholds based on average ingress queue percentage utilization. See in the event history the threshold percentage for queue utilization. Additional capacity may be required to service the traffic load. Contact My Oracle Support for support.

1. Recovery:

- If congestion falls below the clear threshold, this alarm clears. The SBR congestion status exceeds the alarm threshold. Additional capacity may be required to service the traffic load. It is recommended to contact My Oracle Support for assistance.

12007 - SBR active sess binding threshold

Event Type:
SBRA

Description:
The SBR application has exceeded its active Session Binding threshold. The configuration, Maximum active session bindings, is used to calculate the percentage.

Severity:
Minor, Major, Critical

Instance:
Sbr.EvCurrentSessionMetric, SBR

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
sbrActiveSessBindThreshold

Cause:
The SBR active session bindings count exceeds the alarm threshold which means the number of bindings and sessions are more than the configured limits.

Diagnostic Information:
Additional capacity may be required to service the traffic load. View additional information in the event history. Contact My Oracle Support for support.

1. Recovery:

1. If total active session bindings fall below the clear threshold, this alarm clears.
2. Navigate to **CPA**, and then **Configuration**, and then **SBR** to increase the maximum active session bindings configuration if it is too low.

12010 - SBR proc term

Event Type:
SBRA

Description:
The SBR application has stopped.

Severity:
Minor, Major, Critical

Instance:
<Sbr>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
pfeSbrProcTermNotify

Cause:
The SBR process monitored by the process manager has terminated. This should cause a switch over of the standby SBR server to active.

Diagnostic Information:

- Look for additional information in the event history.
- Contact My Oracle Support (MOS) for support.

1. Recovery:

- When an active SBR is terminated as indicated by this alarm, its standby becomes active. The Process Manager automatically attempts to restart the terminated process. If the Process Manager fails to start the terminated process, it raises the alarm again. The standby that became active remains active until it is placed into standby mode again.
  1. Check the status of the terminated SBR by navigating to **Status & Manage**, and then **Server**.
  2. If the Process Manager cannot restart the process, it is recommended to contact My Oracle Support for assistance.

33730 - U-SBR database audit statistics report

Event Type
I-SBR

Description
U-SBR database audit statistics report.

Severity
Info

Instance
<SbrSgName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
ipfeSbrProcTermNotify

1. Recovery

- This report provides statistics related to Universal SBR table audits. Each SBR server generates this event upon reaching the last record in a table. The statistics reported are appropriate for the type of table being audited.

vSTP Alarms and Events (70000-70060, 70100-70999)

70000 - Association Down

Alarm Group
vSTP

Description
Association down

Severity
Major

Instance
<AssocName>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpassociationDownNotify

1. Recovery
1. If the association is manually disabled, then no further action is needed.
2. Verify the association's local IP address and port number are configured on the remote ASP.
3. Verify the association's remote IP address and port are correctly identify a remote ASP.
4. Verify that IP network connectivity exists between the MP server and the remote ASP.
5. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
6. Verify the remote ASP is not under maintenance.
7. It is recommended to contact My Oracle Support for assistance if needed

70001 - Link Down

Alarm Group
vSTP

Description
Link down

Severity
Minor

Instance
<LinkName>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPLinkDownNotify

1. Recovery

1. This alarm indicates that an MTP2 link is not in **In-Service** state. Generally this alarm is asserted when a server or the network is undergoing maintenance or when a link has been manually disabled.
2. If the E1/T1 trunk hosting the link or the link itself is manually disabled, then no further action is necessary.
3. Verify that TimeSlot and LinkSpeed are configured properly.
4. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
5. Verify that the remote E1/T1 trunk is not under maintenance.
6. It is recommended to contact My Oracle Support for assistance if needed

70002 - RSP/Destination Unavailable

Alarm Group
vSTP

Description
HLRR is unable to access the SS7 Destination Point Code because the RSP status is Unavailable.

Severity
Critical

Instance
<RSPName> (of the RSP/Destination which failed)

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3RouteUnavailableNotify

1. Recovery

1. If the RSP/Destination becomes Unavailable due to a Linkset failure, the M3UA attempts to automatically recover all links not manually disabled or blocked.

2. If the RSP/Destination becomes Unavailable due to the receipt of a TFP, MTP3 periodically audits the route's status by sending an RSP message to the adjacent point code which sent the TFP.
3. It is recommended to contact My Oracle Support for assistance if needed

70003 - RSP/Destination Route Unavailable

Alarm Group
vSTP

Description
HLRR is unable to access the SS7 Destination Point Code using this route.

Severity
Minor

Instance
<RouteName>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3RouteUnavailableNotify

1. Recovery

1. If the route becomes Unavailable due to a Linkset failure, the M3UA attempts to automatically recover all links not manually disabled or blocked.
2. If the route becomes Unavailable due to the receipt of a TFP, MTP3 periodically attempts to validate the route using the MTP3 signaling-route-set-test procedure.
3. It is recommended to contact My Oracle Support for assistance if needed

70004 - Linkset Unavailable

Alarm Group
vSTP

Description
The SS7 linkset to an adjacent SP has failed.

Severity
Major

Instance
<LinkSetName>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3LinksetUnavailableNotify

1. Recovery
1. M3UA attempts to automatically recover all links not manually disabled or blocked.
2. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
3. Verify the adjacent server is not under maintenance.
4. It is recommended to contact My Oracle Support for assistance if needed

70005 - Link Unavailable

Alarm Group
vSTP

Description
M3UA has reported to MTP3 that a link is out of service.

Severity
Minor

Instance
<LinkName>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3LinkUnavailableNotify

1. Recovery
1. M3UA attempts to automatically recover all links not manually disabled or blocked.
2. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
3. Verify that the adjacent server is not under maintenance.
4. It is recommended to contact My Oracle Support for assistance if needed

70006 - Preferred Route Unavailable

Alarm Group
vSTP

Description
MTP3 has started to utilize a lower priority (higher cost) route to route traffic toward a given destination address because the higher priority (lower cost) route specified for that RSP/Destination has become unavailable.

Severity
Major

Instance
<RSPName>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3PreferredRouteunavailableNotify

1. Recovery

1. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
2. Verify the adjacent server is not under maintenance.
3. It is recommended to contact My Oracle Support for assistance if needed

70007 - Node Isolated - All Links Down

Alarm Group
vSTP

Description
Node isolated - All links down.

Severity
Major

Instance
<None>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3NodeIsolatedAllLinkDownNotify

1. Recovery

1. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
2. Verify the adjacent server is not under maintenance.

3. It is recommended to contact My Oracle Support for assistance if needed

70008 - Linkset Restricted

Alarm Group
vSTP

Description
The SS7 linkset to an adjacent SP has restricted.

Severity
Major

Instance
<LinksetName>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3LinksetRestrictedNotify

1. Recovery
1. Check the event history logs at **Alarms & Events**, and then **View History** for additional SS7 events or alarms from this MP server.
2. Verify that the adjacent server is not under maintenance.
3. It is recommended to contact My Oracle Support for assistance if needed.

70009 - Link Congested

Alarm Group
vSTP

Description
Link congested

Severity
Minor, Major, Critical

Instance
<LinkName>

HA Score
Normal

Auto Clear Seconds
N/A

OID
vSTPMtp3LinkCongestionNotify

1. Recovery
   The percent utilization of the VSTP's link congestion is approaching its maximum capacity. If this problem persists and the queue reaches 100% utilization based on the level defined, alarm is generated.

   This alarm should not normally occur when no other congestion alarms are asserted. This may occur for a variety of reasons:

   - An IP network or Adjacent node problem may exist preventing SCTP from transmitting messages into the network at the same pace that messages are being received from the network.
   - The SCTP Association may be experiencing a problem preventing it from processing events from its event queue.

1. Examine the alarm logs from **Main Menu > Alarms & Events**.
2. If one or more MPs in a server site have failed, the traffic will be distributed amongst the remaining MPs in the server site. MP server status can be monitored from **Main Menu > Status & Control > Server Status**.
3. There may be an insufficient number of MPs configured to handle the network traffic load. The egress traffic rate of each MP can be monitored from **Main Menu > Status & Control > KPI Display**. If all MPs are in a congestion state then the offered load to the server site is exceeding its capacity.
4. It is recommended to contact My Oracle Support for assistance if needed.

70050 - SCTP Connection Refused

Alarm Group
vSTP

Description
SCTP connection refused.

Severity
Info

Instance
<Link>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPSctpConnectionRefusedNotify

1. Recovery

- Recheck the configured IP Address of the remote node. It is recommended to contact My Oracle Support for assistance if needed.

70051 - Failed to Configure Transport

Alarm Group
vSTP

Description
Failed to configure Transport.

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPFailedtoconfigureConnectionNotify

1. Recovery

- An association is configured each time the association is established. If association configuration fails, it is recommended to contact My Oracle Support for assistance if needed.

70052 - Far-end Closed the Connection

Alarm Group
vSTP

Description
Far-end closed the connection.

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPFarendclosedtheconnectionNotify

1. Recovery
1. Investigate the remote node is failed or if it is under maintenance.

2. Check the remote node for alarms or logs that might indicate the cause for their closing the association.
3. It is recommended to contact My Oracle Support for assistance if needed.

70053 - SCTP Connection Closed

Alarm Group
vSTP

Description
SCTP connection closed.

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPSctpconnectionclosedNotify

1. Recovery
1. Verify IP network connectivity still exists between the MP server and the remote server.
2. Verify the remote server is not configured to change IP addresses once connection is established.
3. Check the event history logs at **Alarms & Events**, and then **View History** to determine if the SCTP Association is experiencing a problem preventing it from processing events from its event queue.
4. Verify the adjacent server is not under maintenance.
5. It is recommended to contact My Oracle Support for assistance if needed

70054 - Remote IP Address State Change

Alarm Group
vSTP

Description
Remote IP Address state change

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPRemoteIPAddressstatechangeNotify

1. Recovery

1. Verify IP network connectivity still exists between the MP server and the remote server.
2. It is recommended to contact My Oracle Support for assistance if needed.

70055 - Association Admin State Change

Alarm Group
vSTP

Description
Association admin state change.

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPAssociationadminstatechangeNotify

1. Recovery

- No action is necessary if this was an expected change due to some maintenance activity. Otherwise, examine security logs on the SO server to determine which user changed the administrative state.

70056 - Link Admin State Change

Alarm Group
vSTP

Description
Link admin state change

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPLinkadminStateChangeNotify

1. Recovery

- No action is necessary if this was an expected change due to some maintenance activity. Otherwise, examine security logs on the SO server to determine which user changed the administrative state.

70057 - Received Invalid M3UA Message

Alarm Group
vSTP

Description
Received invalid M3UA message.

Severity
Info

Instance
<AssociationName>, <LinkName>, or <LinkId>

HA Score
Normal

Throttle Seconds
10

OID
vSTPVstpReceivedinvalidM3UAMessageNotify

1. Recovery

- Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the malformed message.
  - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
  - Error code 0x03 indicates an unsupported M3UA message class.
  - Error code 0x04 indicates an unsupported M3UA message type.
  - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
  - Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.

- Error code 0x12 indicates a parameter field error. Parameter is malformed (such as invalid length).
- Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and Protocol Error are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
- Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
- Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.

70058 - Received M3UA ERROR

Alarm Group
vSTP

Description
Received M3UA ERROR.

Severity
Info

Instance
If message can be mapped to a link, then <LinkName>. Otherwise, <AssociationName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPVstpReceivedM3uaErrorNotify

1. Recovery

- Examine the M3UA error code and the diagnostic information and attempt to determine why the far-end of the link sent the ERROR message.
  - Error code 0x01 indicates an invalid M3UA protocol version. Only version 1 is supported.
  - Error code 0x03 indicates an unsupported M3UA message class.
  - Error code 0x04 indicates an unsupported M3UA message type.
  - Error code 0x05 indicates an unsupported M3UA traffic mode.
  - Error code 0x07 indicates an M3UA protocol error. The message contains a syntactically correct parameter that does not belong in the message or occurs too many times in the message.
  - Error code 0x09 indicates an invalid SCTP stream identifier. A DATA message was sent on stream 0.

- Error code 0x0D indicates that the message was refused due to management blocking. An ASP Up or ASP Active message was received, but refused for management reasons.
- Error code 0x11 indicates an invalid parameter value. Parameter type and length are valid, but value is out of range.
- Error code 0x12 indicates a parameter field error. Parameter is malformed (such as invalid length).
- Error code 0x13 indicates an unexpected parameter. Message contains an undefined parameter. The differences between this error and Protocol Error are subtle. Protocol Error is used when the parameter is recognized, but not intended for the type of message that contains it. Unexpected Parameter is used when the parameter identifier is not known.
- Error code 0x14 indicates that the destination status is unknown. This message can be sent in response to a DAUD from the MP server if the SG cannot or does not wish to provide the destination status or congestion information
- Error code 0x16 indicates a missing parameter. Missing mandatory parameter, or missing required conditional parameter.
- Error code 0x19 indicates an invalid routing context. Received routing context not configured for any linkset using the association on which the message was received.

70059 - Failed to Send DATA Message

Alarm Group
vSTP

Description
Failed to send DITA message.

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPMtp3TfpReceivedNotify

1. Recovery
1. Check the event history logs at **Alarms & Events**, and then **View History** for additional events or alarms from this MP server.
2. Verify the remote server is not under congestion. The MP server has alarms to indicate the congestion if this is the case.
3. It is recommended to contact My Oracle Support for assistance if needed.

70060 - TFP Received

Alarm Group:
vSTP

Description:
This event is generated when a TFP message is received by the MTP3 layer.

Severity:
Info

Instance:
None

Throttle Seconds:
30

OID:
vSTPMtp3TfpReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70061 - TFA Received

Event Type:
vSTP

Description:
This event is generated when a TFA message is received by the MTP3 layer.

Severity:
Info

Instance:
None

Throttle Seconds:
30

OID:
vSTPMtp3TfaReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70062 - TFR Received

Alarm Group:
vSTP

Description:
This event is generated when a TFR message is received by the MTP3 layer.

Severity:
Info

Instance:
None

Throttle Seconds:
30

OID:
vSTPMtp3TfrReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70063 - TFC Received

Alarm Group:
vSTP

Description:
This event is generated when a TFC message is received by the MTP3 layer.

Severity:
Info

Instance:
None

Throttle Seconds:
30

OID:
vSTPMtp3TfcReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70064 - MTP3 Routing Error

Alarm Group:
vSTP

Description:
This event is generated when a message was discarded due to a routing error.

Severity:
Info

Instance:
None

Throttle Seconds:
10

OID:
vSTPMtp3RoutingFailureNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70065 - MTP3 Routing Error - Invalid NI

Alarm Group:
vSTP

Description:
This event is generated when a message was discarded due to a routing error - the network indicator value received in a message from the network is not assigned to the MP.

Severity:
Info

Instance:
None

Throttle Seconds:
10

OID:
vSTPMtp3RoutingFailureInvalidNiNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70066 - MTP3 Routing Error - Invalid SI

Alarm Group:
vSTP

Description:
This event is generated when a message was discarded due to a routing error - the SI value received in a message from the network is associated with a User Part that is not currently supported.

Severity:
Info

Instance:
None

Throttle Seconds:
10

OID:
vSTPMtp3RoutingFailureInvalidSiNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70067 - Failed to Receive DATA Message

Alarm Group:
vSTP

Description:
This event is generated when a M3UA discarded a message due to any of the these reasons:

- Invalid Header, Unsupported Message Type
- Invalid Header, Version Invalid
- Invalid Header, Unsupported Message Class
- Invalid Header, Invalid Stream Identifier
- Invalid Header, Length is Invalid
- Message Decode Failed
- Unexpected Message
- Invalid Routing Context
- Unsupported Traffic Mode
- No configured AS for ASP
- Link is Disabled

Severity:
Info

Instance:
None

Throttle Seconds:
10

OID:
vSTPFailedToReceiveDataMessageNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70068 - vSTP EIR Application Status Changed

Alarm Group:
vSTP

Description:
ComAgent service is unavailable or congested.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
86400

OID:
vSTPVstpEirApplDegradedNotify

1. Make sure the UDR connection is up and the ComAgent service is up and not degraded.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70069 - TCAP Invalid Parameter or Decode Failure

Alarm Group:
vSTP

Description:
Failed to decode TCAP parameter.

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
10

OID:
vSTPVstpEirTcapDecodeErrNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70070 - Message Encode Failed

Alarm Group:
vSTP

Description:
Failed to encode message.

Severity:
Minor

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
10

OID:
vSTPVstpEirEncodeFailNotify

1. Make sure the CGPA parameter is correct.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70071 - Missing IMEI

Alarm Group:
vSTP

Description:
IMEI is missing in the received message

Severity:
Minor

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
1800

Throttle (Seconds):
3600

OID:
vSTPVstpMissingImeiNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70072 - Invalid IMEI Length

Alarm Group:
vSTP

Description:
Invalid length for map IMEI parameter.

Severity:
Minor

Instance:
None

HA Score:
Normal

Throttle (Seconds):
86400

OID:
vSTPVstpMissingImeiNotify

1. Make sure the IMEI is a valid length.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70073 - Unsupported TCAP Message Type

Alarm Group:
vSTP

Description:
Unsupported TCAP message type.

Severity:
Minor

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0

Throttle (Seconds):
10

OID:
vSTPVstpInvalidImeiNotify

1. Make sure the TCAP message type is correct.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70075 - vSTP LSS Stack Event Queue Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the VSTP MP's LSS Stack Event Queue is approaching its maximum capacity.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
86400

OID:
vSTPVstpLssEventQueueNotify

1. Make sure stack queue utilization comes back to 50/70/90 percent.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70076 - vSTP Logging Stack Event Queue Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the VSTP MP's Logging Stack Event Queue is approaching its maximum capacity.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
86400

OID:
vSTPVstpLssLoggingEventQueueNotify

1. Make sure stack queue utilization comes back to 50/70/90 percent.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70077 - vSTP EIR Log Fetch Error

Alarm Group:
vSTP

Description:
EIR log copy from MP to SOAM has failed.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
86400

OID:
vSTPVstpEirApplLogFetchErrorNotify

1. Make sure the SOAM is able to copy the EIR logs from SOAM.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70078 - vSTP EIR Logging Error in MP

Alarm Group:
vSTP

Description:
Log write error in MP.

Severity:
Major

Instance:
Normal

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
10

OID:
vSTPVstpEirLogErrorNotify

1. Look for errors in the MP logs.
2. It is recommended to contact My Oracle Support if further assistance is needed.

70079 - M3UA Ingress Message Discarded

Alarm Group:
vSTP

Description:
This event is generated when vSTP discards an M3UA ingress message for any of these reasons:

- Invalid Header
- Message Decode Failed
- Unexpected Message, AspInactive received in Invalid State
- Invalid Routing Context
- Received message in Invalid state
- Unsupported Traffic Mode
- Unexpected Message, link state is not active
- No configured AS for ASP
- Unexpected Message, AspPayload received in Invalid State
- Unexpected Message, AspDaud received in Invalid State
- Unexpected Message, AspActive is received in Invalid state
- Link is Disabled
- Unexpected Message, AspUp is received in Invalid state
- Message length is greater than 272 bytes

Severity:
Info

Instance:
None

Throttle Seconds:
10

OID:
vSTPM3uaIngressMsgDiscardedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70081 - vSTP M3RL Linkset Buffer Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the VSTP MP's M3RL Linkset Buffer is approaching its maximum capacity.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear
0 (zero)

Throttle Seconds:
86400

OID:
vSTPM3rlLinksetBufferUtilNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70082 - vSTP M3RL RSP Buffer Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the VSTP MP's M3RL Rsp Buffer is approaching its maximum capacity.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear
0 (zero)

Throttle Seconds:
86400

OID:
vSTPM3rlRspBufferUtilNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70083 - vSTP M2PA Retransmission Buffer Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the VSTP MP's M2PA Retransmission Buffer Buffer is approaching its maximum capacity.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear
0 (zero)

Throttle Seconds:
86400

OID:
vSTPM2paRetransmissionBufferUtilNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70084 - vSTP MTP2 Transmission and Retransmission Buffer Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the VSTP MPs MTP2 Transmission and Retransmission Buffer is approaching its maximum capacity.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear
0 (zero)

Throttle Seconds:
86400

OID:
vSTPMtp2TransmissionBufferUtil

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70091 - Missing Mandatory Parameter

Alarm Group:
vSTP

Description:
Mandatory parameter is missing in the received message.

Severity:
Minor

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds):
10

OID:
VstpMissingMandatoryParm

1. Recovery:

1. xxx
2. It is recommended to contact My Oracle Support if further assistance is needed.

70092 - Malformed Subscriber ID

Alarm Group:
vSTP

Description:
This event is generated when the subscriber ID paramenter length is less than or greater than 2 plus the length of MSISDN.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpMalformedSubId

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70093 - Unexpected Value for Subscriber ID

Alarm Group:
vSTP

Description:
This event is generated when the choice for subscriber identity is not MSISDN.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpUnexpectedSubId

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70094 - Invalid MSISDN Length

Alarm Group:
vSTP

Description:
This event is generated when there is an invalid length for the MSISDN value in the subscriber identity parameter.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpInvalidMsisdn

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70095 - ATINP Invalid Requested Info

Alarm Group:
vSTP

Description:
This event is generated when an invalid requested information parameter is in the ATI query message.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpInvalidRequestedInfo

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70096 - Digits Truncated in Encoded Parameter

Alarm Group:
vSTP

Description:
This event is generated when digits are truncated in the encoded parameter of the response message.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpDigitsTruncated

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70100 - ATINP Application Status Changed

Alarm Group:
vSTP

Description:
ATINP application state has changed to one of these states:

- available
- unavailable
- degraded

This alarm is raised when the UDR connection or CA service is down or degraded.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
300

OID:
N/A

1. Recovery:

- This alarm clears when the UDR connection is back up or the CA service is available again.

70101 - Transmission Association Queue Congestion Crossed

Alarm Group:
vSTP

Description:
vSTP egress connection message queue utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<AssocName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
vSTPVstpTxConnQueueCongestedNotify

1. Recovery:

1. Determine if an IP network or Adjacent node problem exists, preventing SCTP from transmitting messages into the network at the same pace that messages are being received from the network.
2. Check the event history logs at **Alarms & Events**, and then **View History** to determine if the SCTP Association is experiencing a problem preventing it from processing events from its event queue..
3. Monitor the MP server status at **Status & Manage**, and then **Server** to determine if one or more MPs in a server site have failed, causing traffic to be distributed amongst the remaining MPs in the server site.
4. Monitor the egress traffic rate of each MP at **Status & Manage**, and then **KPIs** to determine if there is an insufficient number of MPs configured to handle the network traffic load..
5. It is recommended to contact My Oracle Support for assistance if needed

70102 - MTP3 Ingress Link MSU TPS Crossed

Alarm Group:
vSTP

Description:
vSTP ingress link MSU TPS threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<Link>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
vSTPVstpRxLinkTpsNotify

1. Recovery:

1. The percent utilization of the vSTP's ingress message traffic coming from the signaling link. The Ingress control servers the vSTP defense and offers a protection against traffic floods or Denial of Service type of attacks.
2. It is recommended to contact My Oracle Support for assistance if needed

70103 - MTP3 Egress Link MSU TPS Crossed

Alarm Group:
vSTP

Description:
vSTP egress link MSU TPS threshold crossed.

Severity:
Minor, Major, Critical

Instance:
<Link>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
vSTPVstpTxLinkTpsNotify

1. Recovery:

1. The percent utilization of the vSTP's egress message traffic coming from the signaling link. The Egress control is meant to protect the network to protect the network elements connected to the STP.
2. It is recommended to contact My Oracle Support for assistance if needed.

70104 - MTP3 Ingress Link Management TPS Crossed

Alarm Group
vSTP

Description
vSTP ingress link TPS threshold crossed for Network management messages

Severity
Critical

Instance
<Link>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpRxMgmtLinkTpsNotify

1. Recovery

1. The percent utilization of the vSTP's ingress management message coming from the signaling link. The ingress control servers the vSTP defense and offers a protection against traffic floods or Denial of Service type of attacks.
2. It is recommended to contact My Oracle Support for assistance if needed.

70105 - Transmission Association Queue Discard Crossed

Alarm Group
vSTP

Description
vSTP egress connection message is discard threshold crossed.

Severity
Minor, Major, Critical

Instance
<AssocName>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpTxDiscardLevelNotify

1. Recovery

1. Determine if an IP network or Adjacent node problem exists, preventing SCTP from transmitting messages into the network at the same pace that messages are being received from the network.
2. Check the event history logs at **Alarms & Events**, and then **View History** to determine if the SCTP Association is experiencing a problem preventing it from processing events from its event queue.
3. Monitor the MP server status at **Status & Manage**, and then **Server** to determine if one or more MPs in a server site have failed, causing traffic to be distributed amongst the remaining MPs in the server site.
4. Monitor the egress traffic rate of each MP at **Status & Manage**, and then **KPIs** to determine if there is an insufficient number of MPs configured to handle the network traffic load.
5. It is recommended to contact My Oracle Support for assistance if needed.

70107 - vSTP SCCP Stack Event Queue Utilization

Alarm Group
vSTP

Description
The percent utilization of the vSTP MP's SCCP Stack Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpSccpStackEventQueueUtilNotify

1. Recovery

- The alarm is an indication of SCCP Stack Event queue utilization is exceeding its configured capacity. It is recommended to contact My Oracle Support for assistance if needed

70108 - vSTP M3RL Stack Event Queue Utilization

Alarm Group
vSTP

Description
The percent utilization of the vSTP MP's M3RL Stack Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpM3rlStackEventQueueUtilNotify

1. Recovery

- The alarm is an indication of M3RL Stack Event queue utilization is exceeding its configured capacity. It is recommended to contact My Oracle Support for assistance if needed

70109 - vSTP M3RL Network Management Event Queue Utilization

Alarm Group
vSTP

Description
The percent utilization of the vSTP MP's M3RL Network Management Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpM3rlNetMgmtEventQueueUtilNotify

1. Recovery

- The alarm is an indication of M3RL Network Management Event queue utilization is exceeding its configured capacity. It is recommended to contact My Oracle Support for assistance if needed

70110 - vSTP M3UA Stack Event Queue Utilization

Alarm Group
vSTP

Description
The percent utilization of the vSTP MP's M3UA Stack Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpM3uaStackEventQueueUtilNotify

1. Recovery

- The alarm is an indication of M3UA Stack Event queue utilization is exceeding its configured capacity. It is recommended to contact My Oracle Support for assistance if needed

70111 - vSTP M2PA Stack Event Queue Utilization

Alarm Group
vSTP

Description
The percent utilization of the vSTP MP's M2PA Stack Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpM2paStackEventQueueUtilNotify

1. Recovery

- The alarm is an indication of M2PA Stack Event queue utilization is exceeding its configured capacity. It is recommended to contact My Oracle Support for assistance if needed

70112 - vSTP M3UA Tx Stack Event Queue Utilization

Alarm Group:
vSTP

Description:
The percent utilization of the vSTP MP's M3UA Tx Stack Event Queue is approaching its maximum capacity.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
vSTPVstpM3uaTxStackEventQueueUtilNotify

1. Recovery:

1. The alarm is an indication of M3UA Tx Stack Event queue utilization is exceeding its configured capacity.
2. It is recommended to contact My Oracle Support for assistance if needed.

70201 - M2PA link operational state changed

Alarm Group:
vSTP

Description:
M2PA link operational state changed

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
vSTPLinkOpStateChangedNotify

1. Recovery:

- No action necessary.

70202 - M2PA Link Failed

Alarm Group:
vSTP

Description:
M2PA link failed

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
vSTPLinkFailedNotify

1. Recovery:

- No action necessary.

70203 - M2PA Ingress Message Discarded

Alarm Group:
vSTP

Description:
M2PA Ingress message discarded

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPIngressMessageDiscardedNotify

1. Recovery:

- No action necessary.

70204 - M2PA Egress Message Discarded

Alarm Group:
vSTP

Description:
M2PA Egress message discarded

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPEgressMessageDiscardedNotify

1. Recovery:

- No action necessary.

70205 - M2PA Message Encoding Failed

Alarm Group:
vSTP

Description:
M2PA Message Encoding Failed

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPMessageEncodeFailedNotify

1. Recovery:

- No action necessary.

70206 - M2PA Message Decoding Failed

Alarm Group:
vSTP

Description:
M2PA Message Decoding Failed

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPMessageDecodeFailedNotify

1. Recovery:

- No action necessary.

70207 - M2PA Proving Period Timer Expired

Alarm Group:
vSTP

Description:
This event is generated when the M2PA proving or proving emergency period timer (T4) expires.

Severity:
Info

Instance:
<Link Name>

Auto Clear Seconds:
10

OID:
vSTPProvingTimerExpiredNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70208 - M2PA Remote Congestion Timer(T6) Expired

Alarm Group:
vSTP

Description:
This event is generated when the M2PA remote timer (M6) expires.

Severity:
Info

Instance:
<Link Name>

Auto Clear Seconds:
10

OID:
vSTPRemoteCongTimerExpiredNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70209 - Received Remote Processor Outage

Alarm Group:
vSTP

Description:
This event is generated when a remote processor outage is received on a M2PA link.

Severity:
Info

Instance:
<Link Name>

Auto Clear Seconds:
10

OID:
vSTPRpoReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70210 - Received Remote Out of Service

Alarm Group:
vSTP

Description:
This event is generated when a remote out of service is received on a M2PA link.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPRemoteOOSReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70220 - MTP2 Link admin state change

Event Group:
vSTP

Description:
This event is generated if the MTP2 link administrative state is manually changed from one administrative state to another (e.g. Disabled to Enabled and vice versa).

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2LinkAdmStateChangeNotify

1. Recovery:

- This event is shows that Link Admin State is changing from one state to another. It is recommended to contact My Oracle Support for assistance, if needed.

70221 - Failed to send message to TDM driver

Event Group:
vSTP

Description:
This event is generated when sending message to TDM driver fails.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2FailedToSendMsgNotify

1. Recovery:

- None. This event is shows that sending message to TDM driver fails. It is recommended to contact My Oracle Support for assistance, if needed.

70222 - Failed to receive message from TDM driver

Event Group:
vSTP

Description:
This event is generated when receive message from TDM driver fails.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2FailedToRcvMsgNotify

1. Recovery:

- None. This event is showing that receive message from TDM driver fails. It is recommended to contact My Oracle Support for assistance, if needed.

70223 - MTP2 link operational state changed

Event Group:
vSTP

Description:
This event is generated when MTP2 link operational state is changed

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2LinkOpStateChangeNotify

1. Recovery:

- This event is shows that MTP2 link operational state is changed from one state to another. It is recommended to contact My Oracle Support for assistance, if needed.

70224 - MTP2 link failed

Event Group:
vSTP

Description:
This event is generated when MTP2 link is failed due to Link Out Of Service Message Received from peer or MTP2 Link Stop Request Received.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2LinkFailedNotify

1. Recovery:

- This event shows that MTP2 link has failed. It is recommended to contact My Oracle Support for assistance, if needed.

70225 - MTP2 Ingress message discarded

Event Group:
vSTP

Description:
This event is generated when MTP2 Ingress message is discarded.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2IngressMsgDiscardedNotify

1. Recovery:

- This event shows that MTP2 Ingress message is discarded. It is recommended to contact My Oracle Support for assistance, if needed.

70226 - MTP2 Egress message discarded

Event Group:
vSTP

Description:
This event is generated when MTP2 Egress message is discarded.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2EgressMsgDiscardedNotify

1. Recovery:

- This event shows that MTP2 Egress message is discarded. It is recommended to contact My Oracle Support for assistance, if needed.

70227 - Received Remote Out Of Service on MTP2 link

Event Group:
vSTP

Description:
This event is generated when Remote Out Of Service is received from peer on MTP2 link.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPMtp2RemoteOOSReceivedNotify

1. Recovery:

- This event shows that Remote Out Of Service is received from peer. It is recommended to contact My Oracle Support for assistance, if needed.

70251 - Subsystem Congested

Alarm Group:
vSTP

Description:
Subsystem congested.

Instance:
DPC = SSN

Severity:
Major

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds)
86400

OID:
vSTPSubSystemCongestedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70252 - Subsystem Prohibited

Alarm Group:
vSTP

Description:
Subsystem prohibited.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds)
86400

OID:
vSTPSubSystemProhibitedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70210 - Received Remote Out of Service

Alarm Group:
vSTP

Description:
This event is generated when a remote out of service is received on a M2PA link.

Severity:
Info

Instance:
<Link name>

Auto Clear Seconds:
10

OID:
vSTPRemoteOOSReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70271 - SCCP Received Invalid Message

Alarm Group
vSTP

Description;
SCCP received invalid message.

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPSccpInvalidMessageReceivedNotify

1. Recovery:

- No action necessary.

70272 - SCCP Message Translation Failed

Alarm Group:
vSTP

Description:
SCCP message translation failed.

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPSccpTranslationFailedNotify

1. Recovery:

- No action necessary.

70273 - SCCP Message Routing Failed

Alarm Group:
vSTP

Description:
SCCP Message Routing Failed

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPSccpMessageRoutingFailedNotify

1. Recovery:

- No action necessary.

70274 - SGMG Message Invalid

Alarm Group:
vSTP

Description:
SGMG message invalid.

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPScmgMessageInvalidNotify

1. Recovery:

- No action necessary.

70275 - GTT SCCP Loop Detected

Alarm Group:
vSTP

Description:
GTT SCCP loop detected.

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPGttSccpLoopDetectedNotify

1. Recovery:

- No action necessary.

70276 - GTT Load Sharing Failed

Alarm Group:
vSTP

Description:
GTT load sharing failed.

Severity:
Info

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
10

OID:
vSTPGttLoadSharingFailedNotify

1. Recovery:

- No action necessary.

70277 – GTT Action Discard MSU

Alarm Group:
vSTP

Description:
The event is generated when the GTT action (for example, DISCARD, UDTS, or TCAP ERROR) is performed and the UIM required flag is set to *Yes* for the GTT Action managed object.

Severity:
Info

Instance:
Combination of *Action Set Name:Action Name*

Auto Clear Seconds:
10

OID:
vSTPVstpGTTActionDiscardedMSUNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70278 – GTT Action Failed

Alarm Group:
vSTP

Description:
The event is generated when the GTT action (for example, DUPLICATE, FORWARD, or TCAP ERROR) has failed.

Severity:
Info

Instance:
Combination of *Action Set Name:Action Name*

Auto Clear Seconds:
10

OID:
vSTPVstpGTTActionFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70279 – GTT MBR Duplicate Set Type Failed

Alarm Group:
vSTP

Description:
This event is generated when the translation duplicate set type encountered and fallback option is *NO*.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpGTTFlobrDupSetTypeFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70280 – GTT MBR Duplicate Set Type Warning

Alarm Group:
vSTP

Description:
This event is generated when the translation duplicate set type encountered and fallback option is *YES*.

Severity:
Info

Instance
None

Auto Clear Seconds:
10

OID:
vSTPVstpGTTFlobrDupSetTypeWarningNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70281 – GTT FLOBR Duplicate Set Name Failed

Alarm Group:
vSTP

Description:
This event is generated when the translation duplicate set type encountered and fallback option is *NO*.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpGTTFlobrDupSetNameFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70282 - GTT FLOBR Duplicate Set Name Warning

Alarm Group:
vSTP

Description:
This event is generated when the translation duplicate set type encountered and fallback option is *YES*.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpGTTFlobrDupSetNameWarningNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70283 - GTT FLOBR Max Search Depth Failed

Alarm Group:
vSTP

Description:
This event is generated after the maximum depth search if the translation is not successful and fallback is *NO*.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpGTTFlobrMaxSearchDepthFailedNotify

1. Recovery:

1. xxx
2. It is recommended to contact My Oracle Support if further assistance is needed.

70284 - GTT FLOBR Max Search Depth Warning

Alarm Group:
vSTP

Description:
This event is generated after the maximum depth search if the translation is not successful and fallback is *YES*.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID
vSTPVstpGTTFlobrMaxSearchDepthWarningNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70285 – MBR Decoding Failed

Alarm Group:
vSTP

Description:
This event is generated when any of these conditions occur:

- Unsupported SCCP Type
- ITU TCAP decoding fails
- Sequence Tag parameter is missing
- Unsupported Component Type
- Unsupported MAP Opcode received
- Unsupported MAP version received
- Unsupported TCAP Package Type
- Mandatory parameter is missing (Target MS)
- Mandatory parameter is missing (Sub Identity)
- Mandatory parameter is missing
- Invalid MAP digits
- IMSI decoding failed
- MSISDN decoding failed

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpMBRDecodeFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70286 - GTT Duplicate Action Processing Stopped

Event Type:
vSTP

Description:
GTT Duplicate Action processing stopped.

Severity:
Major

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0

OID:
vSTPDuplicateActionInhibitNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70291 - XUDT UDT Conversion Failed.

Alarm Group:
vSTP

Description:
This event is generated when an XUDT UDT conversion fails.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpXudtUdtConversionFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70292 - SCCP Encode Failure

Alarm Group:
vSTP

Description:
SCCP encode failure is generated when these occur:

- Invalid GTI
- Unsupported GTI
- Invalid Data Message length
- Invalid Optional Portion Length

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpSccpEncodeFailedNotify

1. Recovery:

- It is recommended to contact My Oracle Support for assistance if needed.

70293 - SFAPP Decode Error

Event Group
vSTP

Description
None

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappDcdErrorNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70294 - SFAPP Validation Matching State not found

Event Group
vSTP

Description
SFAPP Validation Matching State not found

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappTIDNotFoundNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70295 - SFAPP Validation Encoding Error

Event Group
vSTP

Description
SFAPP Validation Encoding Error

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappEcdErrorNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70296 - SFAPP Validation Response Timeout Error

Event Group
vSTP

Description
SFAPP Validation Response Timeout Error

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappRspTimeoutNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70297 - SFAPP Validation Velocity Chk Failed.

Event Group
vSTP

Description
SFAPP Validation Velocity Chk Failed.

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappThreshExcdNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70298 - SFAPP Validation Failed

Event Group
vSTP

Description
SFAPP Validation Failed

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappValidationFailedNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70299 - SFAPP Invalid CC/NDC received

Event Group
vSTP

Description
SFAPP Invalid CC/NDC received

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPSfappInvalidCCNDCreceivedNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70300 - Updation failed in UDR

Event Group
vSTP

Description
Updation failed in UDR

Severity
Major

Instance
None

HA Score
Normal

OID
vSTPVstpUpdationFailedinUDRNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70301 - VSTP SFAPP Stack Event Queue Utilization

Alarm Group:
vSTP

Description:
This event is generated when the percent utilization of the vSTP MP's SFAPP Event Queue is approaching its maximum capacity.

Severity:
Major

Instance:
None

Auto Clear Seconds:
0

OID:
vSTPSfappEventQueueUtilNotify

- The event is cleared when the percent utilization of the VSTP MP's SFAPP Event Queue comes back to normal. It is recommended to contact My Oracle Support if further assistance is needed.

70302 - Invalid Length of Conditioned Digits

Alarm Group:
vSTP

Description:
This event is generated when the MNP length of the conditioned digit is invalid.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpSrvcInvDgtLenNotify

1. xxx
2. It is recommended to contact My Oracle Support if further assistance is needed.

70303 - Conv to Intl Num - Dflt NC Not Found

Alarm Group:
vSTP

Description:
This event is generated when NC is not defined

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpSrvcDfltNcNotDfnNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70304 - MNP Circular Route Detected

Alarm Group:
vSTP

Description:
This event is generated when a loop is detected

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpGportLoopDetectedNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70305 - Translation PC Type is ANSI

Alarm Group:
vSTP

Description:
This event is generated when the MNP translated PC type is ANSI.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpPcTypeAnsiNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70306 - Invalid Digits in MAP MSISDN Parameter

Alarm Group:
vSTP

Description:
This event is generated when there is an invalid MSISDN for SRI or SRISM.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpInvMsisdnDgtNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70307 - Invalid Prefix/Suffix Digit Length

Alarm Group:
vSTP

Description:
This event is generated when the prefix/suffix digit length is more than 21 digits.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpSrvcInvPrefxLenNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70308 - Translation PC is Local Point Code

Alarm Group:
vSTP

Description:
This event is generated when MNP is xlated to EAGLE TPC.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpSrvcXlatedPcIsEagleTpcNotify

- It is recommended to contact My Oracle Support if further assistance is needed.

70309 - ANSI Translation Not Supported

Alarm Group:
vSTP

Description:
This event is generated when MNP CGPA GTA xlation is crossing the domain.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpSccpRtnXingDomainNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70310 - Too many digits for DRA parameter

Event Group
vSTP

Description
DRA digits have exceeded INAP_MAX_CDPN_DIGITS (32)

Severity
Major

Instance
None

HA Score
Normal

OID
VstpTooManyDigitDRA

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70311 - IDPR CGPN encoding failed

Event Group
vSTP

Description
Failed to encode the CGPN for IDPR Feature

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIdprCgpnEcdError

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70312 - IDPR CDPN encoding failed

Event Group
vSTP

Description
Failed to encode the CDPN for IDPR Feature

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIdprCdpnEcdError

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70313 - IDPRCDPN(X) NPP SERVICE is OFF

Event Group
vSTP

Description
IDPRCDPN(X) NPP SERVICE is OFF

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIdprCdpnNppServiceOff

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70314 - IDPRCGPN NPP SERVICE is OFF

Event Group
vSTP

Description
IDPRCGPN NPP SERVICE is OFF

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIdprCgpnNppServiceOff

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70315 - DESTINATION ADDRESS DECODING is FAIL

Event Group
vSTP

Description
DESTINATION ADDRESS DECODING is FAIL

Severity
Major

Instance
None

HA Score
Normal

OID
VstpDestAddrDcdFail

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70316 - TCAP ENCODING is FAIL

Event Group
vSTP

Description
TCAP ENCODING is FAIL

Severity
Major

Instance
None

HA Score
Normal

OID
VstpTcapEncFail

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70317 - OUT OF BOUND DIGIT

Event Group
vSTP

Description
OUT OF BOUND DIGIT

Severity
Major

Instance
None

HA Score
Normal

OID
VstpOutBoundDigit

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70318 - SMS MANDATORY PARAMETER MISSING

Event Group
vSTP

Description
SMS MANDATORY PARAMETER MISSING

Severity
Major

Instance
None

HA Score
Normal

OID
VstpSMSMandParamMiss

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70319 - ADDRESS DECODING is FAIL

Event Group
vSTP

Description
ADDRESS DECODING is FAIL

Severity
Major

Instance
None

HA Score
Normal

OID
VstpAddrDcdFail

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70320 - MNPCDPA MATCHES HOME SMSC

Event Group
vSTP

Description
MNPCDPA MATCHES HOME SMSC

Severity
Major

Instance
None

HA Score
Normal

OID
VstpMnpCdpaMatchHomeSmsc

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70331 - SCCP XUDT Reassembly Failure

Event Group
vSTP

Description
SCCP XUDT Reassembly Failure

Severity
Major

Instance
None

HA Score
Normal

OID

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70332 - SCCP XUDT Segmentation Failure

Event Group
vSTP

Description
SCCP XUDT Segmentation Failure

Severity
Major

Instance
None

HA Score
Normal

OID

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70351 – vSTP Maintenance Leader HA Notification to Go Active

Alarm Group:
vSTP

Description:
This event is generated when vSTP has received a notification from HA that the Maintenance Leader resource should transition to the Active role.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpMpLeaderGoActiveNotificationNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70352 – vSTP Maintenance Leader HA notification to GO OOS

Alarm Group:
vSTP

Description:
This event is generated when vSTP received a notification from HA that the Maintenance Leader resource should transition to the OOS role.

Severity:
Info

Instance:
None

Auto Clear Seconds:
1

OID:
vSTPVstpMpLeaderGoOOSNotificationNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70353 – Routing DB Inconsistency Exists

Alarm Group:
vSTP

Description:
vSTP routing DB inconsistencies exist among the DA-MPs in the DSR signaling NE.

Severity:
Critical

Instance:
Table Name

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds)
86400

OID:
vSTPVstpRoutingDbInconsistencyExistsNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70354 – vSTP DB Table Monitoring Overrun

Alarm Group:
vSTP

Description:
This event is generated when a vSTP DB table monitoring overrun has occurred. The COMCOL update synchronization log used by DB Table monitoring to synchronize routing DB among all DA-MP RT-DBs has overrun. The vSTP-MPs routing DB sharing table is automatically audited and re-synchronized to correct any inconsistencies.

Severity:
Info

Instance:
<Table Name>

Auto Clear Seconds:
1

OID:
vSTPVstpTblMonCbOnLogOverrunNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70355 - vSTP DB Table Monitoring Error

Alarm Group:
vSTP

Description:
This event is generated when an unexpected error occurred during DB table monitoring.

Severity:
Info

Instance:
<Thread Name>

Auto Clear Seconds:
10

OID:
vSTPVstpSldbMonAbnormalErrorNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70356 - Failed to Process Ingress MSU: Peer MP Unavailable or Congested

Alarm Group:
vSTP

Description:
This event is generated when the egress STP MP is unavailable or congested.

Severity:
Info

Instance:
<Ingress STP-MP hostname>

Auto Clear Seconds:
1

OID:
vSTPPeerMPUnavlblOrCngstedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70371 - No vSTP-MP Leader Detected

Alarm Group:
vSTP

Description:
This event is generated when:

- no active vSTP-MP leaders are reported by the maintenance leader
- there is a single vSTP-MP and the DSR process is stopped
- there are multiple vSTP-MPs, the DSR process is stopped, and there is a ComAgent connection failure between two or more vSTP-MPs.

Severity:
Info

Instance:
<Network Element>

Auto Clear Seconds:
10

OID:
vSTPNoVstpMpLeaderDetectedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70372 - Multiple vSTP-MP Leader Detected

Alarm Group:
vSTP

Description:
This event is generated when:

- more than one vSTP-MP reports themselves as leader.
- the DSR process is running on all vSTP-MPs and the ComAgent connection is down between two or more DA-MPs

The alarm clears when the maintenance leader reports a single active DA-MP leader.

Severity:
Info

Instance:
<Network Element>

Auto Clear Seconds:
10

OID:
vSTPMultipleVstpMpLeadersDetectedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70373 - Connection Alarm Aggregation Threshold Reached

Alarm Group:
vSTP

Description:
This event is generated when there are a critical number of fixed connection alarms for the vSTP-MP.

Severity:
Info

Instance:
<vSTP-MP-Hostname>

Auto Clear Seconds:
10

OID:
vSTPConnectionAlarmAggregationThresholdReachedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70374 - Link Alarm Aggregation Threshold Reached

Alarm Group:
vSTP

Description:
This event is generated when the number of critical link alarms for a single network element exceeds the configurable alarm threshold.

Severity:
Info

Instance:
<Network Element>

Auto Clear Seconds:
10

OID:
vSTPLinkAlarmAggregationThresholdReachedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70375 - Linkset Alarm Aggregation Threshold Reached

Alarm Group:
vSTP

Description:
This event is generated when the number of critical linkset alarms for a single network element exceeds the configurable alarm threshold.

Severity:
Info

Instance:
<Network Element>

Auto Clear Seconds:
10

OID:
vSTPLinksetAlarmAggregationThresholdReachedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70376 - Route Alarm Aggregation Threshold Reached

Alarm Group:
vSTP

Description:
This event is generated when the number of critical route alarms for a single network element exceeds the configurable alarm threshold.

Severity:
Info

Instance:
<Network Element>

Auto Clear Seconds:
10

OID:
vSTPRouteAlarmAggregationThresholdReachedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70377 - RSP Alarm Aggregation Threshold Reached

Alarm Group:
vSTP

Description:
This event is generated when the number of critical RSP alarms for a single network element exceeds the configurable alarm threshold

Severity:
Info

Instance:
<Network Element>

Auto Clear Seconds:
10

OID:
vSTPRspAlarmAggregationThresholdReachedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70378 - SLTC Failure

Alarm Group:
vSTP

Description:
This event is generated when vSTP is unable to complete the signaling link test message exchange due to any of these reasons:

- No Response
- Invalid Point Code (DPC)
- No route to APC on linkset
- Invalid Point Code (OPC)
- Invalid Linkset
- Bad data patteren
- Invalid SLC

Severity:
Minor

Instance:
<Link Name>

Auto Clear Seconds:
10

OID:
vSTPSltcFailureInvalidSlcNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70379 - Unexpected TFA Received

Alarm Group:
vSTP

Description:
This event is generated when vSTP receives an unexpected TFA message due to any of these reasons:

- TFA received for Unknown Affected Point Code
- TFA is not generated from the adjacent node
- No Route Configured to Affected Point Code using linkset

- Duplicate TFA message received

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPUnexpectedTfaReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70380 - Unexpected TFR Received

Alarm Group:
vSTP

Description:
This event is generated when vSTP receives an unexpected TFR message due to any of these reasons:

- TFR is not supported for ITUI domain
- TFR received for Unknown Affected Point Code
- TFR is not generated from the adjacent node
- No Route configured for Affected Point Code using linkset
- Duplicate TFR Received

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPUnexpectedTfrReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70381 - Unexpected TFP Received

Alarm Group:
vSTP

Description:
This event is generated when vSTP receives an unexpected TFP message due to any of these reasons:

- TFP received for Unknown Affected Point Code
- TFP is not generated from the adjacent node
- No Route configured for Affected Point Code using linkset
- Duplicate TFP Received

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPUnexpectedTfpReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70382 - Unexpected TFC Received

Alarm Group:
vSTP

Description:
This event is generated when vSTP receives an unexpected TFC message due to any of these reasons:

- TFC received with congestion level 0
- TFC received for Unknown Affected Point Code
- TFC received for Unavailable Affected Point Code

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPUnexpectedTfcReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70383 - Invalid H0 H1 Code

Alarm Group:
vSTP

Description:
This event is generated when vSTP finds an invalid H0 or H1 code in the message due to any of these reasons:

- Invalid H0 code
- Invalid H1 code

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPInvalidH0H1CodeNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70384 - TFC Generated

Alarm Group:
vSTP

Description:
This event is generated when vSTP generates a TFC message for congested point code.

Severity:
Info

Instance:
None

Throttle Seconds:
10

OID:
vSTPTfcGeneratedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70385 - Change Over Order Performed

Alarm Group:
vSTP

Description:
This event is generated when vSTP performs a changeover.

Severity:
Info

Instance:
<Link Name>

Auto Clear Seconds:
10

OID:
vSTPReceivedCOONotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70386 - Emergency Change Over Performed

Event Type:
vSTP

Description:
This event is generated when vSTP performs an emergency changeover.

Severity:
Info

Instance:
<Link Name>

Auto Clear Seconds:
10

OID:
vSTPECOPerformedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70387 - Changeback Timer Expired

Alarm Group:
vSTP

Description:
This event is generated when the changeback timer (for example, T5 timer) expires.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPCbTimerExpiredNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70388 - UPU Received

Alarm Group:
vSTP

Description:
This event is generated when vSTP receives a user part unavailable (USP) message due to any of these reasons:

- SCCP user unavailable, cause unknown
- User part is not SCCP

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPUpuReceivedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70389 - Remote Blocked

Alarm Group:
vSTP

Description:
Remote blocked.

Severity:
Minor

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds)
86400 (this is a latched alarm so 1-day throttling has the same effect as the old LcEcon)

OID:
vSTPRemoteBlockedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70290 - RSP/Destination Restricted

Alarm Group:
vSTP

Description:
Limited access to the SS7 Destination Point Code because the RSP status is restricted.

Severity:
Minor

Instance:
<RSP Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

Throttle (Seconds)
86400 (this is a latched alarm so 1-day throttling has the same effect as the old LcEcon)

OID:
vSTPMtp3RspRestrictedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70391 - RSP/Destination Route Restricted

Alarm Group:
vSTP

Description:
Limited access to the SS7 destination point code using this route because its restricted.

Severity:
Minor

Instance:
<Route Name>

HA Score:
Minor

Auto Clear Seconds:
0 (zero)

Throttle (Seconds)
86400 (this is a latched alarm so 1-day throttling has the same effect as the old LcEcon)

OID:
vSTPMtp3RouteRestrictedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70392 - MSU Failed MTP Screening

Alarm Group:
vSTP

Description:
This event is generated when an MSU was discarded due to screening.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpMsuDiscardDueToScrNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70411 - ANSI to ITU CDPA GT Conversion Failure

Alarm Group:
vSTP

Description:
This event generates when vSTP receives an ANSI to ITU CDPA GT conversion falure. This happens when an entry in the default GT Conversion Table could not be found to match the incoming ANSI message's Translation Type in the Calling Party Address parameter when the GTCNVDFLT M3rl option is not enabled.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpAICdTtMismatchNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70401 - ANSI to ITU CGPA GT Conversion Failure

Alarm Group:
vSTP

Description:
This event generates when vSTP receives an ANSI to ITU CGPA GT conversion falure. This happens when an entry in the default GT Conversion Table could not be found to match the incoming ANSI message's Translation Type in the Calling Party Address parameter when the GTCNVDFLT M3rl option is not enabled.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpAICgTtMismatchNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70402 - ITU to ANSI CDPA GT Conversion Failure

Alarm Group:
vSTP

Description:
An entry in the default GT Conversion Table could not be found to match the incoming ITU message's NP/NAI/TT in the Called Party Address parameter when the GTCNVDFLT M3rl Option is not enabled.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpIACdTtMismatchNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70403 - ITU to ANSI CGPA GT Conversion Failure

Alarm Group:
vSTP

Description:
This event is generated when an entry in the default GT Conversion Table could not be found to match the incoming ITU message's NP/NAI/TT in the Calling Party Address parameter when the GTCNVDFLT M3rl Option is not enabled.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpIACgTtMismatchNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70404 - Affected PC Conversion Failure

Alarm Group:
vSTP

Description:
This event is generated when no alias PC of the destination type for the affected point code is found.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpAftPcCnvFailNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70404 - OPC Conversion Failed

Alarm Group:
vSTP

Description:
This event is generated when no alias PC of the destination network type for the OPC is found.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpM3rlOpcCnvFailNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70406 - Conversion Failed. CGPA PC Alias Undefined

Alarm Group:
vSTP

Description:
This event is generated when no alias PC of the destination network type for the CGPA PC is found, and the discard CGPA PC option for the destination network type is off.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpCgPcAlsUndefinedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70407 - Conversion MSU Discard. SCCP MSU Too Large

Alarm Group:
vSTP

Description:
This event is generated when the SCCP MSU total length after conversion is greater than supported message length.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpInvMsgLengthNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70408 - Conversion MSU Discard. Invalid Segmentation Parameters

Alarm Group:
vSTP

Description:
This event is generated when the segmentation optional parameter length is incorrect for the message undergoing ANSI/ITU SCCP conversion.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpInvSegParLengthNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70409 - Conversion Failed. Incorrect SCCP Parameter Length

Alarm Group:
vSTP

Description:
This event is generated when a message error is found during the encoding of SCCP message due to incorrect CDPA, CGPA, or SCCP data message parameter length.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpInvSccpEleLenErrorNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70410 - MTP3 Circular Loop Detected

Alarm Group:
vSTP

Description:
This event is generated when an incloming linkset and outgoing message linkset is same; or when the OPC in the message is configured as self PC for the MTP routed message.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpmtp3LoopDetectedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70411 - Conversion MSU Discard. Invalid SCMG Message Type

Alarm Group:
vSTP

Description:
This event is generated when the SCMG message type is invalid.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpInvScmgMsgTypeNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70416 - SCCP Application MSU Discarded

Alarm Group:
vSTP

Description:
This event is generated when the CPC type is not STP and the application is not provisioned for that CPC type.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
vSTPVstpSCCPAppMSUDiscardedNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70418 - Sccp Egress Tps Threshold Crossed

Alarm Group
vSTP

Description
Sccp Egress Tps Threshold Crossed.

Severity
Major

Instance
<AssocName>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpSccpEgressTpsThresholdNotify

1. Recovery

- It is recommended to contact My Oracle Support for assistance if needed

70420 - Unsupported ACN Object ID Length

Alarm Group:
vSTP

Description:
This event is generated when an ACN object identifier length is greater than 32.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpInvAcnLenNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70421 - Failed to Decode TCAP Parameters

Alarm Group:
vSTP

Description:
This event is generated when there is an invalid INAP Called Party Number and no parameter sequence.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpFailtoDecodeInapParamNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70422 - INAP Called Party Number is Missing

Alarm Group:
vSTP

Description:
This event is generated when the INAP Called Party Number is missing.

Severity:
Info

Instance:
None

Auto Clear Seconds:
10

OID:
VstpFailtoDecodeInapParamNotify

1. Recovery:

- It is recommended to contact My Oracle Support if further assistance is needed.

70423 - Unexpected SI in TIF Stop Action

Event Group
vSTP

Description
Unexpected SI in TIF Stop Action

Severity
Major

Instance
None

HA Score
Normal

OID
VstpTifUnexpectedSi

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70424 - Modified MSU too large to route

Event Group
vSTP

Description
Modified MSU too large to route

Severity
Major

Instance
None

HA Score
Normal

OID
VstpTifRouteFailed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70425 - ISUP IAM Decode Failed

Event Group
vSTP

Description
ISUP IAM Decode Failed

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIsupDcdFailed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70425 - ISUP IAM Decode Failed

Event Group
vSTP

Description
ISUP IAM Cld Pty decode failed

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIsupDcdCdpaFailed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70427 - ISUP Encode Failed

Event Group
vSTP

Description
ISUP Encode Failed

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIsupEcdFailed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70428 - TIF CgPN NS Failure: CC mismatch in DN

Event Group
vSTP

Description
TIF CgPN NS Failure: CC mismatch in DN

Severity
Major

Instance
None

HA Score
Normal

OID
VstpIsupEcdFailed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70429 - VLR Status changed

Event Group
vSTP

Description
VLR Status changed

Severity
Major

Instance
None

HA Score
Normal

OID
VstpDynVlrStatusChanged

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70430 - Velocity Threshold Crossed

Event Group
vSTP

Description
Velocity Threshold Crossed

Severity
Major

Instance
None

HA Score
Normal

OID
VstpDynVeloThreshCrossed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70431 - Dynamic VLR Profile Aging

Event Group
vSTP

Description
Dynamic VLR Profile Aging

Severity
Major

Instance
None

HA Score
Normal

OID
VstpDynVLRProfAging

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70432 - Dynamic VLR Roaming Aging

Event Group
vSTP

Description
Dynamic VLR Roaming Aging

Severity
Major

Instance
None

HA Score
Normal

OID
VstpDynVLRRoamAging

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70433 - Vstp Dynamic learning is turned OFF

Event Group
vSTP

Description
Vstp Dynamic learning is turned OFF

Severity
Major

Instance
None

HA Score
Normal

OID
VstpVlrDynLearningOFF

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70434 - Vstp Dynamic learning LEARN Mode Timer Expired

Event Group
vSTP

Description
Vstp Dynamic learning LEARN Mode Timer Expired

Severity
Major

Instance
None

HA Score
Normal

OID
VstpVlrDynLearningLearntimer

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70435 - Vstp Dynamic learning Profile Table Full

Event Group
vSTP

Description
Vstp Dynamic learning Profile Table Full

Severity
Major

Instance
None

HA Score
Normal

OID
VstpVlrDynProfileTableFull

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70436 - Vstp Dynamic learning Roaming Table Full

Event Group
vSTP

Description
Vstp Dynamic learning Roaming Table Full

Severity
Major

Instance
None

HA Score
Normal

OID
VstpVlrDynProfileTableFull

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70437 - VSTP Security Logging Stack Event Queue Utilization

Event Group
vSTP

Description
The percent utilization of the VSTP MP's Security Logging Stack Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

OID
VstpSecuLogEventQueue

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70438 - Vstp Security Logging Error in MP

Event Group
vSTP

Description
vSTP error in logging security logs to csv file in MP.

Severity
Major

Instance
None

HA Score
Normal

OID
VstpSecuLogError

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70439 - Vstp Security Log Fetch Error

Event Group
vSTP

Description
Vstp Security Log File fetching from MP failed.

Severity
Major

Instance
None

HA Score
Normal

OID
VstpSecuLogFetchError

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70440 - Vstp Security Log Fetch Error at Remote Server

Event Group
vSTP

Description
Vstp Security Log File fetching from Active SO to Remote Server failed.

Severity
Major

Instance
None

HA Score
Normal

OID
VstpSecuLogRemoteServerError

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70446 - VstpServiceStackEventQueueUtil

Alarm Group
vSTP

Description
The percent utilization of the VSTP MPs Service Stack Event Queue is approaching its maximum capacity.

Severity
Major

Instance
None

HA Score
Normal

OID

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70451 - serviceMpUnavailable

Alarm Group
vSTP

Description
Service MP not available, can't send message to Service Mp.

Severity
Major

Instance
None

HA Score
Normal

OID
VstpSecuLogRemoteServerError

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70458 - Transaction Not Found for Ack.

Event Group
vSTP

Description
Ack Message for which Transaction are not found in both Originator and Termination Side at Service MP

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyAckTransNotFnd

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70454 - SMS Proxy SCCP Validation Failed

Event Group
vSTP

Description
SCCP Validation failed in Service MP due to inconsistency between sccp cdpa and tcap smrpda

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxySccpValidFail

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70448 - SMS Proxy Message Validation Response Timeout Error

Event Group
vSTP

Description
Service Validation Response Timeout Error

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyValRspTimeout

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70447 - Service Validation Failed

Event Group
vSTP

Description
SMS Proxy Message Validation Failed

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyValidationFailed

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70450 - SMS Proxy Message Validation Encoding Error

Event Group
vSTP

Description
Service Validation Encoding Error

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyEcdError

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70450 - Service Validation Decoding Error

Event Group
vSTP

Description
SMS Proxy Message Validation Decoding Error.

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyDcdErrort

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70453 - SMS Proxy GT address blocked

Event Group
vSTP

Description
Service SMSC Blocklist

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyBlocklist

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70452 - SMS Proxy GT address allowed.

Event Group
vSTP

Description
Service SMSC Allowlist

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyAllowlist

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70456 - Serivce DOS Timer Timeout

Event Group
vSTP

Description
DOS Timer waits for Delivery Report SM message and on timeout raises this event

Severity
Major

Instance
None

HA Score
Normal

OID
Vstp smsProxyDosInvkTimeout

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

70455 - Service MTFSM Invoke Timer Timeout.

Event Group
vSTP

Description
MTFSM Invoke Timer waits for MTFSM message and on timeout raises this event

Severity
Major

Instance
None

HA Score
Normal

OID
smsProxyMtfsmInvkTimeout

1. Recovery

- It is recommended to contact My Oracle Support for assistance, if needed.

Diameter Equipment Identity Register (EIR) (71000-71999)

71000 - EIR Message Decoding Failure

Event Type
Event

Description
EIR application failed to decode the request.

Severity
N/A

Instance
MP hostname

HA Score
Normal

Throttle Seconds
10

OID
N/A

- Make sure the length of the IMEI and IMSI numbers are correct.

71001 - ECA Routing Attempt Failed

Event Type
Event

Description
ECA routing attempt failed due to DRL queue exhaustion.

Severity
N/A

Instance
MP hostname

HA Score
Normal

Throttle Seconds
10

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

71002 - EIR Message Encoding Failure

Event Type
Event

Description
EIR application failed to encode the answer.

Severity
N/A

Instance
MP hostname

HA Score
Normal

Throttle Seconds
10

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

71003 - EIR Application Unavailable

Event Type
Alarm

Description
EIR Application is Unavailable.

Severity
Critical

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- Enable the EIR application as the administrator.

71004 - UDR DB Connection Error

Event Type
Alarm

Description
ComAgent connection between DSR EIR and UDR is down.

Severity
Critical

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

71005 - EIR TPS Exceeded

Event Type
Alarm

Description
The Message rate is exceeding the supported TPS for DSR EIR application.

Severity
Minor/Major/Critical

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

71006 - EIR Logging Suspended

Event Type
Alarm

Description
The DSR EIR Logging is suspended.

Severity
Major

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

1. Make sure the log file and directory are still accessible.
2. Make sure there is enough disk space for the log file.

71007 - EIR Request Queue Utilization

Event Type
Alarm

Description
EIR request queue utilization threshold exceeded.

Severity
Minor/Major/Critical

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- Increase the EIR request queue utility threshold.

71008 - EIR UDR Response Queue Utilization

Event Type
Alarm

Description
EIR UDR response queue utilization threshold exceeded.

Severity
Minor/Major/Critical

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- Increase the EIR request queue utility threshold.

71009 - EIR Application Congested

Event Type
Alarm

Description
EIR Application is congested.

Severity
Major

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

71010 - ComAgent Registration Failure

Event Type
Alarm

Description
ComAgent routing service registration or service notification registration failed, EIR cannot use the ComAgent service for database queries.

Severity
Critical

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

71011 - Fetch Log Failed at SO

Event Type
Alarm

Description
Fetching of EIR logs failed at SO.

Severity
Major

Instance
MP hostname

HA Score
Normal

Throttle Seconds
86400

OID
NA

- It is recommended to contact My Oracle Support for assistance if needed.

4
Key Performance Indicators (KPIs)

This section provides general information about **KPI**s and lists the KPIs that can appear on the Status & Manage > KPIs GUI page.

General KPIs information

This section provides general information about KPIs, the **Status and Manage**, and then **KPIs** page, and how to view KPIs.

KPIs Overview

Key Performance Indicators (KPIs) allow you to monitor system performance data, including CPU, memory, swap space, disk space, shared memory, and uptime per server. This performance data is collected from all servers within the defined topology.

The KPI display function resides on all OAM servers. Servers that provide a GUI connection rely on KPI information merged to that server. The Network OAMP servers maintain status information for all servers in the topology. System OAM servers have reliable information only for servers within the same network element.

The Status and Manage KPIs page displays performance data for the entire system. KPI data for the entire system is updated every 60 seconds. If data is not currently being collected for a particular server, the KPI for that server will be shown as N/A.

KPIs

The **Status & Manage**, and then **KPIs** page displays KPIs for the entire system. KPIs for the server and its applications are displayed on separate tabs. The application KPIs displayed may vary according to whether you are logged in to an NOAM server or an SOAM server.

KPIs Server Elements

This table describes KPIs that display regardless of server role.

Table 4-1 KPIs Server Elements

KPIs Status Element	Description
Network Element	The network element name, which is set up on the **Configuration**, and then **Network Elements** page, associated with each Server Hostname.
Server Hostname	The server hostname set up on the **Configuration**, and then **Servers** page. All servers in the system are listed here.
Server Indicators	

Table 4-1 (Cont.) KPIs Server Elements

KPIs Status Element	Description
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system.
RAM	Percentage utilization of physical memory on the server by all software as measured by TPD.
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.
Disk	Percentage utilization of disk space on the server by all software as measured by the operating system.
ShMem	Percentage utilization of shared memory on the server by all software as measured by the operating system.
Uptime	The total amount of time the server has been running.

Viewing KPIs

Use this procedure to view KPI data.

1. Navigate to **Status & Manage**, and then **KPIs**.

   For details about the KPIs displayed on this page, see the application documentation.

2. Click **KPI Filter** and specify filter options to see KPI data relevant to an application.

3. Click **Go** to filter on the selection.

> **Note:**
>
> The application KPIs displayed may vary according to whether you are logged in to an NOAM server or an SOAM server. Collection of KPI data is handled solely by NOAM servers in systems that do not support SOAMs.

KPIs data export elements

This table describes the elements on the KPIs > Export page.

Table 4-2 Schedule KPI Data Export Elements

Element	Description	Data Input Notes
Export Frequency	Frequency at which the export occurs	Format: Radio button Range: Fifteen Minutes, Hourly, Once, Weekly, or Daily Default: Once
Task Name	Name of the scheduled task	Format: Textbox Range: Maximum length is 40 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Task Name must begin and end with an alphanumeric character.
Description	Description of the scheduled task	Format: Textbox Range: Maximum length is 255 characters; alphanumeric (a-z, A-Z, and 0-9) and minus sign (-). Description must begin with an alphanumeric character.
Minute	If hourly or fifteen minutes is selected for Upload Frequency, this is the minute of each hour when the data will be written to the export directory.	Format: Scrolling list Range: 0 to 59 Default: 0
Time of Day	Time of day the export occurs	Format: Time textbox Range: 15-minute increments Default: 12:00 AM
Day of Week	Day of week on which the export occurs	Format: Radio button Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting KPIs

You can schedule periodic exports of security log data from the KPIs page. KPI data can be exported immediately, or you can schedule exports to occur daily or weekly. If filtering has been applied in the KPIs page, only filtered data is exported.

During data export, the system automatically creates a CSV file of the filtered data. The file will be available in the file management area until you manually delete it, or until the file is transferred to an alternate location using the **Export Server** feature. For more information about using Export Server, see Data Export.

> **Note:**
>
> When a KPI is exported to a CSV file, each KPI column name is prefixed with an appropriate Group name. For example, KPI related to Diameter is displayed as `[Diameter]MsgCopy Queue Utilization`.

Use this procedure to schedule a data export task.

1. Select **Status & Manage**, and then **KPIs**.
2. If necessary, specify filter criteria and click **Go**.

   The KPIs display according to the specified criteria.
3. Click **Export**.
4. Enter the **Task Name**.

   For more information about **Task Name**, or any field on this page, see KPIs data export elements.
5. Select the **Export Frequency**.
6. If you selected Hourly, specify the Minutes.
7. Select the **Time of Day**.

   > **Note:**
   >
   > **Time of Day**is not an option if**Export Frequency** equals**Once**.
8. Select the **Day of Week**.

   > **Note:**
   >
   > **Day of Week** is not an option if **Export Frequency** equals **Once**.
9. Click **OK** or **Apply** to initiate the KPI export task.

   From the **Status & Manage**, and then **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see View the File List.

   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage**, and then **Tasks**. For more information see:

   - Editing a Scheduled Task
   - Deleting a Scheduled Task
   - Generating a Scheduled Task Report

Computer Aided Policy Making (CAPM) KPIs

The KPI values associated with CAPM are available using **Status & Manage**, and then **KPIs**.

Table 4-3 CAPM KPIs

Variable	Description
Processing time [µSEC]	Average processing time (in microseconds) of Rule Template on a per Rule Template basis.
Active Templates	Number of Rule Templates that are in Active state.
Test Templates	Number of Rule Templates that are in Test state.
Development Templates	Number of Rule Templates that are in Development state.
Match Rule	References one element in the arrayed measurement.

Communication Agent (ComAgent) KPIs

The KPI values associated with ComAgent are available using **Status & Manage**, and then **KPIs**.

Table 4-4 Communication Agent KPIs

Variable	Description
User Data Ingress message rate	The number of User Data Stack Events received by ComAgent.
Broadcast Data Rate	The overall data broadcast rate on the server.

DCA Custom MEAL KPIs

The KPI values associated with DCA are visible using **Status & Manage**, and then **KPIs**. There are 25 scalar basic templates, 25 scalar Rate templates, 25 arrayed Basic templates, and 25 arrayed Rate templates.

Table 4-5 DCA Custom MEAL KPIs

Variable	Description
DcaCustomMeal.name	DcaCustomMeal.kpiDescr

DCA Framework KPIs

The KPI values associated with DCA are visible using **Status & Manage**, and then **KPIs**.

Table 4-6 DCA Framework KPIs

Variable	Description
Ingress Message Rate	Average Ingress Message Rate (messages per second) of Diameter messages received by the DCA Application
U-SBR Query Rate	Average U-SBR Query Rate (Stack Events per second successfully sent to the U-SBR
Runtime Errors Rate	Instant Runtime Error Rate (runtime errors per second during the last sampling interval)
U-SBR Query Failure Rate	Average rate of ComAgent errors encountered when attempting to send an U-SBR query
Transactions Error Answer	Diameter transactions that a DCA App relay answers with error
Completed Transactions	Diameter transactions that a DCA App successfully relays
Transactions Discard Request	Diameter transactions that a DCA App terminates by discarding the request
Max Perl Main Opcodes	Maximum number of opcodes executed by the Perl script main part
Max Perl Handler Opcodes	Maximum number of opcodes executed by the Perl script event handlers
Opcode Quota Exceed	Diameter transactions that a DCA App terminates per second because the maximum number of opcodes is exceeded

Diameter (DIAM) KPIs

The KPI values associated with Diameter are available using **Status & Manage**, and then **KPIs**.

Table 4-7 DIAM KPIs

Variable	Description
MsgCopyTxQueueUtilization	Percentage of utilization of the Message Copy Tx Queue
Average Response Time	The average time from when routing receives a request message from a peer to when routing sends an answer message to that peer.
Transaction Success Rate	Percentage of Diameter and RADIUS transactions successfully completed on a DA-MP server with respect to the offered load.

DP KPIs

Table 4-8 DP KPIs

Variable	Description
DpsQueryRate	Total number of queries received per second

Table 4-8 (Cont.) DP KPIs

Variable	Description
DpsMsisdnQueryRate	Total number of MSISDN queries received per second
DpsImsiQueryRate	Total number of IMSI queries received per second
DpsNaiQueryRate	Total number of NAI queries received per second
DpsExtIdQueryRate	The total number of External Identifier Queries Received per second
DpsFailedQueryRate	Total number of queries failed per second
DpsNotFoundQueryRate	Total number of queries with Not Found responses per second
DpsMsisdnNotFoundQueryRate	Total number of MSISDN queries with Not Found responses per second
DpsImsiNotFoundQueryRate	Total number of IMSI queries with Not Found responses per second
DpsNaiNotFoundQueryRate	Total number of NAI queries with Not Found responses per second
DpsNExtIdNotFoundQueryRate	The total number of External Identifier Queries with NotFound Responses per second
DpsResponseSent	Total number of responses sent per second
DpsIngressQueue	DP Ingress Queue percentage full
DpsMsisdnBlacklistedRate	Total number of MSISDN Queries with Blacklisted Responses per second
DpsImsiBlacklistedRate	Total number of IMSI Queries with Blacklisted Responses per second

Equipment Identity Register (EIR) KPIs

The KPI values associated with SCEF are visible using **Status & Manage**, and then **KPIs**.

Table 4-9 Diameter EIR KPIs

Variable Number	Name	Description
20900	RxDeirMsgRate	Incoming ECR rate. Ingress message rate (messages per second) utilization on a MP server for EIR. The ingress message rate is the number of Diameter messages that were successfully received by EIR per second.

Table 4-9 (Cont.) Diameter EIR KPIs

Variable Number	Name	Description
20901	TxDeirMsgRate	Outgoing ECA rate. Egress message rate (messages per second) utilization on a MP server for EIR. The egress message rate is the number of Diameter messages that were successfully sent by EIR per second.
20902	DeirDbQueryRate	UDR DB Query rate. Database query rate EIR. The Database query rate is the number of query sent from EIR to the UDR database per second.
20903	DeirDbSuccessResponseRate	UDR DB success rate. Database response rate for EIR. The Database response rate is the number of successful lookup result received by EIR from UDR database per second.
20904	DeirMsgSuccessRate	EIR success message rate (messages per second) on an MP server. The success message rate is the number of ingress Diameter messages that are processed by EIR and answered with a success (2xxx) result code.
20905	DeirRequestMsgQueue	EIR's Request stack task queue utilization
20906	DeirUdrResponseMsgQueue	EIR's Response stack task queue utilization
20907	DeirLoggingQueue	EIR's Logging stack task queue utilization
20908	DeirLoggingRate	EIR Logging rate

Table 4-10 SS7 EIR KPIs

Variable Number	Name	Description
21030	SS7 EIR Recv Msgs/Sec	SS7 EIR MSUs received per second
21031	SS7 EIR Xmit Msgs/Sec	SS7 MSUs transmitted per second
21032	SS7 EIR DB request rate	SS7 EIR DB Tx rate
21033	SS7 EIR DB response rate	SS7 EIR DB Rx rate

IDIH KPIs

The KPI values associated with the IDIH will be visible via the GUI **Status & Manage**, and then **KPIs**

Table 4-11 IDIH KPIs

Variable	Description
DSR-DIH TTR Bandwidth (KB/sec)	Average bandwidth used by DSR in sending TTRs (including trace start and stop messages) to DIH in Kbytes per second

IP Front End (IPFE) KPIs

The KPI values associated with IPFE are visible using **Status & Manage**, and then **KPIs**.

Table 4-12 IPFE KPIs

Variable	Description
CPU %	Total CPU used by the IPFE process
Memory Total	Absolute memory used by the IPFE process
Memory %	Percent memory used by the IPFE process
Mem. Heap	Total heap allocated by the IPFE process
IPFE Packets/Sec	The average number of packets per second the IPFE receives
IPFE MBytes/Sec	The average number of megabytes per second the IPFE receives

Message Processor (MP) KPIs

The KPI values associated with MP are available using **Status & Manage**, and then **KPIs**.

Table 4-13 MP KPIs

Variable	Description
Avg CPU Utilization	Percentage of CPU utilization by the Diameter process on a DA-MP server.
Offered Load (MPS)	Offered load on a DA-MP server, corresponding to the message rate before policing by capacity and congestion controls.
Accepted Load (MPS)	Accepted load on a DA-MP server, corresponding to the message rate after policing by capacity and congestion controls.

Table 4-13 (Cont.) MP KPIs

Variable	Description
Messsage Processing Load (MPS)	Average message processing load (messages per second) on a MP server. The message processing load is the number of Diameter messages that are routed, including Reroute and MsgCopy.

Full Address Based Resolution (FABR) KPIs

The KPI values associated with FABR are available using **Status & Manage**, and then **KPIs**.

Table 4-14 FABR KPIs

Variable	Description
Ingress Message Rate	Ingress Message Rate (messages per second) utilization on a MP server for the FABR application. The Ingress Message Rate is the number of ingress Diameter messages that were successfully received by the FABR application.
Resolved Message Rate	Resolved Message Rate (messages per second) utilization on a MP server. The Resolved Message Rate is the number of ingress Diameter messages that are successfully resolved to a Destination by the FABR application.
DP Response Time Average	Average DP response time is the average time (in milliseconds) it takes to receive a DP response after sending the corresponding DP query.

Platform KPIs

The KPI values associated with Platform are available using **Status & Manage**, and then **KPIs**.

Table 4-15 Platform KPIs

Variable	Description
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system.
RAM	Percentage utilization of physical memory on the server by all software as measured by TPD.
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.

Table 4-15 (Cont.) Platform KPIs

Variable	Description
Uptime	The total amount of time(days HH:MM:SS) the server has been running.

Policy and Charging Application (PCA) KPIs

The KPI values associated with PCA are available using **Status & Manage**, and then **KPIs**.

Table 4-16 PCA KPIs

Variable	Description
PCA Ingress Message Rate	Number of Diameter messages including both requests and answers received by PCA from the Diameter Routing Layer per second.
P-DRA Ingress Message Rate	Number of Diameter messages including both requests and answers received by P-DRA from the Diameter Routing Layer per second.
OC-DRA Ingress Message Rate	Number of Diameter messages including both requests and answers received by OC-DRA from the Diameter Routing Layer per second.

Process-based KPIs

Table 4-17 Process-based KPIs

Variable	Description
provimport.Cpu	CPU usage of provimport process
provimport.MemHeap	Heap memory usage of provimport process
provimport.MemBasTotal	Memory usage of provimport process
provimport.MemPerTotal	Percent memory usage of provimport process
provexport.Cpu	CPU usage of provexport process
provexport.MemHeap	Heap memory usage of provexport process
provexport.MemBasTotal	Memory usage of provexport process
provexport.MemPerTotal	Percent memory usage of provexport process
pdbrelay.Cpu	CPU usage of pdbrelay process
pdbrelay.MemHeap	Heap memory usage of pdbrelay process
pdbrelay.MemBasTotal	Memory usage of the pdbrelay process
pdbrelay.MemPerTotal	Percent memory usage of pdbrelay process
pdbaudit.Cpu	CPU usage of pdbaudit process
pdbaudit.MemHeap	Heap memory usage of pdbaudit process
pdbaudit.MemBasTotal	Memory usage of the pdbaudit process
pdbaudit.MemPerTotal	Percent memory usage of pdbaudit process
pdba.Cpu	CPU usage of pdba process
pdba.MemHeap	Heap memory usage of pdba process

Table 4-17 (Cont.) Process-based KPIs

Variable	Description
pdba.MemBasTotal	Memory usage of pdba process
pdba.MemPerTotal	Percent memory usage of pdba process
xds.Cpu	CPU usage of xds process
xds.MemHeap	Heap memory usage of xds process
xds.MemBasTotal	Memory usage of xds process
xds.MemPerTotal	Percent memory usage of xds process
dpserver.Cpu	CPU usage of dpserver process on DP
dpserver.MemHeap	Heap memory usage of dpserver process on DP
dpserver.MemBaseTotal	Memory usage of the dpserver process on DP
dpserver.MemPerTotal	Percent memory usage of dpserver on DP
era.Cpu	CPU usage of era process
era.MemHeap	Heap memory usage of era process
era.MemBasTotal	Memory usage of era process
era.MemPerTotal	Percent memory usage of era process

Provisioning KPIs

Table 4-18 Provisioning KPIs

Variable	Description
ProvConnections	The number of provisioning client connections currently established. A single connection includes a client having successfully established a TCP/IP connection, sent a provisioning connect message, and having received a successful response.
ProvMsgsReceived	The number of provisioning messages per second that have been received from all sources except import files.
ProvMsgsImported	The number of provisioning messages per second imported from files.
ProvMsgsSuccessful	The number of provisioning messages per second that have been successfully processed and a success response sent to the requestor.
ProvMsgsFailed	The number of provisioning messages per second that have failed to be processed due to errors and a failure response sent to the requestor.
ProvMsgsSent	The number of provisioning message responses sent per second to the requestor.
ProvMsgsDiscarded	The number of provisioning messages discarded per second. provisioning messages are discarded due to connection shutdown, server shutdown, server‘s role switching from active to standby, or transaction not becoming durable within the allowed amount of time.

Table 4-18 (Cont.) Provisioning KPIs

Variable	Description
ProvTxnCommitted	The number of provisioning transactions per second that have been successfully committed to the database (memory and on disk) on the active server of the primary SDS cluster.
ProvTxnFailed	The number of provisioning transactions per second that have failed to be started, committed, or aborted due to errors.
ProvTxnAborted	The number of provisioning transactions aborted per second.
ProvTxnActive	The number of provisioning transactions that are currently active (normal transaction mode only).
ProvTxnNonDurable	The number of transactions that have been committed, but are not yet durable. Responses for the associated requests are not sent until the transaction has become durable.
ProvRelayMsgsSent	The number of relayed provisioning messages sent per second.
ProvRelayMsgsSuccessful	The number of relayed provisioning messages per second that were successful at the HLRR.
ProvRelayMsgsFailed	The number of relayed provisioning messages per second that failed at the HLRR.
ProvRemoteAuditMsgsSent	The number of IMSI and MSISDN records audited per second.
ProvRelayTimeLag	Time in seconds between timestamps of last record PdbRelay processed and latest entry in the Command Log.
ProvDbException	The number of DB Exception errors per second.

Range Based Address Resolution (RBAR) KPIs

The KPI values associated with RBAR are available using **Status & Manage**, and then **KPIs**.

Table 4-19 RBAR KPIs

Variable	Description
Avg Resolved Message Rate	Average Resolved Message Rate (messages per second) utilization on a MP server. The Resolved Message Rate is the number of ingress Diameter messages that are successfully resolved to a Destination by the RBAR application.

Table 4-19 (Cont.) RBAR KPIs

Variable	Description
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on a MP server for this DSR application. The Ingress Message Rate is the number of ingress Diameter messages that were successfully received by the DSR application.

SCEF KPIs

The KPI values associated with SCEF are visible using **Status & Manage**, and then **KPIs**.

Table 4-20 Non Arrayed KPIs

Variable	Description
NIDD Message Processing Rate	The number of messages processed every second by the NIDD feature of SCEF application
NIDD CMR Message	The total number of NIDD CMR messages processed by the NIDD feature of SCEF application
NIDD NIR Message	The total number of NIDD NIR messages processed by the NIDD feature of SCEF application
NIDD TDR Message	The total number of NIDD TDR messages processed by the NIDD feature of SCEF application
NIDD ODR Message	The total number of NIDD ODR messages processed by the NIDD feature of SCEF application
Monitoring Message Rate	The number of messages processed every second by the Monitoring feature of SCEF application
Enhanced Coverage Message Rate	The number of messages processed every second by the Enhanced Coverage feature of SCEF application
DT Message Processing Rate	The number of messages processed every second by the Device Trigger feature of SCEF application

Table 4-21 Arrayed KPIs

Variable	Description
Monitoring CFG Requests Rate	Rate at which SCS/AS is submitting T8 Monitoring Configuration Requests to SCEF application.
Monitoring RPT Received Rate	Rate at which SCEF application is receiving Monitoring Reports from HSS/MME/SGSN.
SCEF Monitoring NOTIFY Sent Rate	Rate at which SCEF application is sending T8 Monitoring Notifications to Scs/As
Successful NIDD Config	The average number of successful NIDD configurations messages by SCEF application
Failed NIDD Config	The average number of failed NIDD configuration messages by SCEF application
Successful NIDD Downlink Transfer	The average number of successfully transferred NIDD Downlink Data messages by SCEF application

Table 4-21 (Cont.) Arrayed KPIs

Variable	Description
Successfully buffered NIDD Downlink	The average number of successfully buffered NIDD Downlink Data messages by SCEF application
Failed NIDD downlink buffering	The average number buffering failure for NIDD Downlink Data messages by SCEF application
Successful NIDD MO	The average number of successful NIDD Uplink Data messages by SCEF application
Failed NIDD MO	The average number of failed NIDD uplink Data messages by SCEF application
Current NIDD Buffered	The number of buffered NIDD downlink Data messages by SCEF application

SS7/Sigtran KPIs

Table 4-22 SS7/Sigtran KPIs

Variable	Description
SCCP Recv Msgs/Sec	SCCP messages received per second.
SCCP Xmit Msgs/Sec	SCCP messages transmitted per second.
SS7 Process CPU Utilization	The average percent of SS7 Process CPU utilization on an MP server.
Ingress Message Rate	The Ingress Message Rate is the number of non-SNM message that M3UA attempts to queue in the M3RL Stack Event Queue.
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent.
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received.

Subscriber Binding Repository (SBR) KPIs

The KPI values for SBR are visible using **Status & Manage**, and then **KPIs**.

Table 4-23 SBR KPIs

Variable	Description
SBR Memory Utilization	SBR memory utilization (0-100%)
SBR Process CPU Utilization	SBR Process CPU Percent Utilization (0-100%)

Table 4-24 SBR-Binding KPIs

Variable	Description
SBR Policy Bindings (IMSI)	Total number of subscribers with at least one binding (IMSI)
SBR Binding DB Read Rate	Number of SBR Binding DB reads per second
SBR Binding DB Write Rate	Number of SBR Binding DB writes per second

Table 4-24 (Cont.) SBR-Binding KPIs

Variable	Description
SBR Alt Key Bindings (MSISDN)	Total number of subscribers with at least one Alternate Key binding (MSISDN)
SBR Alt Key Bindings (IPv4)	Total number of subscribers with an Alternate Key binding (IPv4)
SBR Alt Key Bindings (IPv6)	Total number of subscribers with an Alternate Key binding (IPv6)

Table 4-25 SBR-Session KPIs

Variable	Description
SBR Policy Sessions	Number of Active SBR Policy Sessions
SBR Policy Session DB Read Rate	Number of SBR Policy Session DB reads per second
SBR Policy Session DB Write Rate	Number of SBR Policy Session DB writes per second
SBR Online Charging Sessions	Number of Active SBR Online Charging Sessions
SBR OC Session DB Read Rate	Number of SBR Online Charging Session DB reads per second
SBR OC Session DB Write Rate	Number of SBR Online Charging Session DB writes per second

U-SBR KPIs

The KPI values associated with Universal SBR are visible using **Status & Manage**, and then **KPIs**.

Table 4-26 U-SBR KPIs

Variable	Description
GenericCreateStateRate	Rate of ingress GenericCreateState stack events messages received by the U-SBR server.
GenericCreateOrReadStateRate	Rate of ingress of GenericCreateOrReadState events processed by the U-SBR Server
GenericReadStateRate	Rate of ingress of GenericReadState events processed by the U-SBR Server
GenericUpdateStateRate	Rate of ingress of GenericUpdateState events processed by the U-SBR Server
GenericConcurrentUpdateStateRate	Rate of ingress of GenericConcurrentUpdateState events processed by the U-SBR Server
GenericDeleteStateRate	Rate of ingress of GenericDeleteState events processed by the U-SBR Server

Table 4-26 (Cont.) U-SBR KPIs

Variable	Description
GenericErrRecObsoletedRate	Rate of received GenericConcurrentUpdateState events by the U-SBR Server that lead to a result event with the error code set to GenericErrRecObsoleted
GenericTotalRequestsRate	Rate of received GenericState events by the U-SBR Server
GenericErrMalformedRequestRate	Rate of Generic State events that could not be decoded by the U-SBR Server
GenericErrRate	Rate of GenericState events that could not be processed by the U-SBR Server and were replied with a GenericErr code

vSTP KPIs

The KPI values associated with Universal SBR are visible using **Status & Manage**, and then **KPIs**.

Table 4-27 vSTP KPIs

Variable	Description
VSTP Process CPU Utilization	Average percent VSTP Process CPU utilization (0-100%) on a MP server
SCCP Xmit Msgs/Sec	SCCP messages transmitted per second
SCCP Recv Msgs/Sec	SCCP messages received per second
M3RL Xmit Msgs/Sec	MTP3 DATA MSUs transmitted per second
M3RL Recv Msgs/Sec	MTP3 DATA MSUs received per second
M3UA Xmit Msgs/Sec	M3UA DATA MSUs transmitted per second
M3UA Recv Msgs/Sec	M3UA DATA MSUs received per second
M2PA Xmit Msgs/Sec	M2PA DATA MSUs transmitted per second
M2PA Recv Msgs/Sec	M2PA DATA MSUs received per second
SS7 EIR Recv Msgs/Sec	EIR Check IMEI received per second
SS7 EIR Xmit Msgs/Sec	EIR Check IMEI response transmitted per second
EIR DB Response Msgs/Sec	EIR DB response received per second
EIR DB Request Msgs/Sec	EIR DB request transmitted per second