Diameter Signaling Router

Alarms and KPIs

Release 8.2

E89015

January 2018

ORACLE

Diameter Signaling Router Alarms and KPIs, Release 8.2

E89015

Copyright © 2011, 2018, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

This documentation is in preproduction status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

1 Introduction

Revision History 1-1
Overview 1-1
Scope and Audience 1-1
Manual Organization 1-1
Documentation Admonishments 1-2
Locate Product Documentation on the Oracle Help Center Site 1-2
Customer Training 1-3
My Oracle Support 1-3
Emergency Response 1-3

2 User Interface Introduction

User Interface Organization 2-1
User Interface Elements 2-2
Main Menu Options 2-5
Missing Main Menu options 2-11
Common Graphical User Interface Widgets 2-11
Supported Browsers 2-11
System Login Page 2-12
Main Menu Icons 2-13
Work Area Displays 2-14
Customizing the Splash Page Welcome Message 2-17
Column Headers (Sorting) 2-17
Page Controls 2-17
Clear Field Control 2-18
Optional Layout Element Toolbar 2-18
Filters 2-20
Pause Updates 2-22
Max Records Per Page Controls 2-22

3 Alarms, Events, and KPIs Overview

Alarms Warning 3-1

General alarms and events information 3-1
Alarms and events overview 3-1
Alarms formatting information 3-3
Alarm and event ID ranges 3-4
Alarm and event types 3-4
Viewing active alarms 3-6
Active alarms data export elements 3-7
Exporting active alarms 3-8
Generating a report of active alarms 3-9
Viewing alarm and event history 3-9
Historical events data export elements 3-10
Exporting alarm and event history 3-11
Generating a report of historical alarms and events 3-12
Viewing the file list 3-13
Opening a file 3-13
Data Export 3-13
Data Export elements 3-13
Configuring data export 3-16
Tasks 3-17
Active Tasks 3-17
Scheduled Tasks 3-20

4 Alarms and Events

IP Front End, IPFE (5000-5999) 4-1
5001 - IPFE Backend Unavailable 4-1
5002 - IPFE address configuration error 4-2
5003 - IPFE state sync run error 4-3
5004 - IPFE IP tables configuration error 4-5
5005 - IPFE Backend In Stasis 4-5
5006 - Error reading from Ethernet device. Restart IPFE process. 4-6
5007 - Out of Balance: Low 4-7
5008 - Out of Balance: High 4-7
5009 - No available servers in target set 4-8
5010 - Unknown Linux iptables command error 4-10
5011 - System or platform error prohibiting operation 4-11
5012 - Signaling interface heartbeat timeout 4-12
5013 - Throttling traffic 4-12
5100 - Traffic Overload 4-13
5101 - CPU Overload 4-14
5102 - Disk Becoming Full 4-14
5103 - Memory Overload 4-15
OAM (10000-10999) 4-16
10000 - Incompatible database version 4-16

10001 - Database backup started 4-16
10002 - Database backup completed 4-17
10003 - Database backup failed 4-17
10004 - Database restoration started 4-18
10005 - Database restoration completed 4-18
10006 - Database restoration failed 4-19
10008 - Database provisioning manually disabled 4-19
10009 - Config and Prov db not yet synchronized 4-20
10010 - Stateful db from mate not yet synchronized 4-20
10011 - Cannot monitor table 4-21
10012 - Table change responder failed 4-21
10013 - Application restart in progress 4-22
10020 - Backup failure 4-22
10050 - Resource Audit Failure 4-23
10051 - Route Deployment Failed 4-23
10052 - Route Discovery Failed 4-24
10053 - Route deployment failed - no available device 4-25
10054 - Device deployment failed 4-25
10055 - Device discovery failed 4-26
10073 - Server Group Max Allowed HA Role Warning 4-27
10074 - Standby server degraded while mate server stabilizes 4-27
10075 - Application processes have been manually stopped 4-28
10078 - Application not restarted on standby server due to disabled failure cleanup mode 4-28
10100 - Log export started 4-29
10101 - Log export successful 4-29
10102 - Log export failed 4-30
10103 - Log export already in progress 4-30
10104 - Log export file transfer failed 4-31
10105 - Log export cancelled - user request 4-32
10106 - Log export cancelled - duplicate request 4-32
10107 - Log export cancelled - queue full 4-33
10108 - Duplicate scheduled log export task 4-33
10109 - Log export queue is full 4-34
10110 - Certificate About to Expire 4-35
10111 - Certificate Expired 4-35
10112 - Certificate Cannot Be Used 4-36
10115 - Health Check Started 4-37
10116 - Health Check Successful 4-37
10117 - Health Check Failed 4-38
10118 - Health Check Not Run 4-38
10120 - Server Group Upgrade Started 4-39
10121 - Server Group Upgrade Cancelled - Validation Failed 4-39

10122 - Server Group Upgrade Successful 4-40
10123 - Server Group Upgrade Failed 4-40
10124 - Server Group Upgrade Cancelled - User Request 4-41
10125 - Server Group Upgrade Failed 4-41
10130 - Server Upgrade Started 4-42
10131 - Server Upgrade Cancelled 4-42
10132 - Server Upgrade Successful 4-43
10133 - Server Upgrade Failed 4-43
10134 - Server Upgrade Failed 4-44
10140 - Site Upgrade Started 4-45
10141 - Site Upgrade Cancelled 4-46
10142 - Site Upgrade Successful 4-46
10143 - Site Upgrade Failed 4-47
10144 - Site Upgrade Cancelled - User Request 4-48
10145 - Site Upgrade Failed 4-48
10151 - Login successful 4-49
10152 - Login failed 4-49
10153 - Logout successful 4-50
10154 - User Account Disabled 4-50
10155 - SAML Login Successful 4-51
10156 - SAML Login Failed 4-51
10200 - Remote database reinitialization in progress 4-52
10300 - SNMP Trapping Not Configured 4-52
IDIH (11500-11549) 4-53
11500 - Tracing Suspended 4-53
11501 - Trace Throttling Active 4-53
11502 - Troubleshooting Trace Started 4-54
11503 - Troubleshooting Trace Stopped 4-54
11506 - Invalid IDIH-Trace AVP 4-55
11507 - Unable to run network trace at this site 4-56
11508 - Network Trace Configuration Error 4-56
11509 - Site Trace Configuration Error 4-57
11510 - Network Trace Activation Error 4-57
11511 - Invalid DIH HostName 4-58
SDS (14000-14999) 4-58
14100 - Interface Disabled 4-58
14101 - No Remote Connections 4-58
14102 - Connection Failed 4-59
14103 - Both Port Identical 4-59
14120 - Connection Established 4-60
14121 - Connection Terminated 4-60
14122 - Connection Denied 4-61
14140 - Import Throttled 4-61

14150 - Import Initialization Failed 4-62
14151 - Import Generation Failed 4-62
14152 - Import Transfer Failed 4-63
14153 - Export Initialization Failed 4-63
14154 - Export Generation Failed 4-64
14155 - Export Transfer Failed 4-65
14160 - Import Operation Completed 4-65
14161 - Export Operation Completed 4-66
14170 - Remote Audit started and in progress 4-66
14171 - Remote Audit aborted 4-67
14172 - Remote Audit failed to complete 4-67
14173 - Remote Audit completed 4-68
14174 - NPA Split pending request deleted 4-68
14175 - NPA Split activation failed 4-69
14176 - NPA Split started and is active 4-69
14177 - NPA Split completion failed 4-70
14178 - NPA Split completed 4-70
14179 - MSISDN deleted from Blacklist 4-71
14180 - IMSI deleted from Blacklist 4-71
14188 - PdbRelay not connected 4-72
14189 - PdbRelay Time Lag 4-72
14198 - ProvDbException 4-73
14200 - DP Stack Event Queue utilization 4-73
14301- ERA Responder Failed 4-74
SS7/Sigtran Alarms (19200-19299) 4-75
19200 - RSP/Destination unavailable 4-75
19201 - RSP/Destination route unavailable 4-76
19202 - Linkset unavailable 4-77
19203 - Link unavailable 4-77
19204 - Preferred route unavailable 4-78
19205 - TFP received 4-79
19206 - TFA received 4-79
19207 - TFR received 4-80
19208 - TFC received 4-80
19209 - M3RL routing error 4-81
19210 - M3RL routing error - invalid NI 4-82
19211 - M3RL routing error - invalid SI 4-83
19217 - Node isolated - all links down 4-83
19226 - Timedout waiting for ASP-UP-ACK 4-84
19227 - Received unsolicited ASP-DOWN-ACK 4-85
19229 - Timed out waiting for ASP-ACTIVE-ACK 4-85
19230 - Received unsolicited ASP-INACTIVE-ACK 4-86
19231 - Received invalid M3UA message 4-87

19233 - Failed to send non-DATA message 4-88
19234 - Local link maintenance state change 4-88
19235 - Received M3UA error 4-89
19240 - Remote SCCP subsystem prohibited 4-90
19241 - SCCP malformed or unsupported message 4-92
19242 - SCCP Hop counter violation 4-92
19243 - SCCP routing failure 4-93
19244 - SCCP routing failure network status 4-94
19245 - SCCP GTT failure 4-94
19246 - Local SCCP subsystem prohibited 4-95
19248 - SCCP Segmentation Failure 4-96
19249 - SCCP Reassembly Failure 4-97
19250 - SS7 process CPU utilization 4-97
19251 - Ingress message rate 4-98
19252 - PDU buffer pool utilization 4-99
19253 - SCCP stack event queue utilization 4-100
19254 - M3RL stack event queue utilization 4-100
19255 - M3RL network management event queue utilization 4-101
19256 - M3UA stack event queue utilization 4-102
19258 - SCTP Aggregate Egress queue utilization 4-103
19259 - Operation discarded due to local resource limitation 4-104
19260 - Transaction could not be delivered to remote TCAP peer due to conditions in the network 4-104
19262 - Operation discarded due to malformed component received from remote TCAP peer 4-105
19263 - Transaction discarded due to malformed dialogue message received from local TC User 4-106
19264 - Transaction discarded due to malformed dialogue message from remote TCAP peer 4-106
19265 - Unexpected event received from local TC User 4-107
19266 - Unexpected event received from remote TCAP peer 4-108
19267 - Dialogue removed by dialogue cleanup timer 4-108
19268 - Operation removed by invocation timer expiry 4-109
19269 - Dialogue aborted by remote TCAP peer 4-110
19270 - Received unsupported TCAP message 4-111
19271 - Operation rejected by remote TCAP peer 4-111
19272 - TCAP active dialogue utilization 4-112
19273 - TCAP active operation utilization 4-113
19274 - TCAP stack event queue utilization 4-114
19275 - Return error from remote TCAP peer 4-114
19276 - SCCP Egress Message Rate 4-115
19281 - TCAP Routing Failure 4-116
Transport Manager Alarms and Events (19400-19419) 4-116

19400 - Transport Down 4-116
19401 - Failed to configure Transport 4-118
19402 - Failed to connect Transport 4-118
19403 - Received malformed SCTP message (invalid length) 4-119
19404 - Far-end closed the Transport 4-120
19405 - Transport closed due to lack of response 4-121
19406 - Local Transport maintenance state change 4-122
19407 - Failed to send Transport DATA Message 4-122
19408 - Single Transport Egress-Queue Utilization 4-123
19409 - Message Rejected by ACL Filtering 4-124
19410 - Adjacent Node IP Address state change 4-125
19411 - SCTP Transport closed due to failure of multihoming validation 4-125
19412 - SCTP Transport configuration mismatched for Adjacent Node IP 4-126
19413 - SCTP Transport closed due to unsupported peer address event recieved 4-126
Communication Agent, ComAgent (19420-19909) 4-127
19420 - BDFQFull 4-127
19421 - BDFThrotl 4-127
19422 - BDFInvalidPkt 4-128
19800 - Communication Agent Connection Down 4-128
19801 - Communication Agent Connection Locally Blocked 4-130
19802 - Communication Agent Connection Remotely Blocked 4-131
19803 - Communication Agent Stack Event Queue Utilization 4-132
19804 - Communication Agent configured connection waiting for remote client to establish connection 4-133
19805 - Communication Agent Failed To Align Connection 4-135
19806 - Communication Agent CommMessage Mempool Utilization 4-136
19807 - Communication Agent User Data FIFO Queue Utilization 4-137
19808 - Communication Agent Connection FIFO Queue utilization 4-137
19810 - Communication Agent Egress Message Discarded 4-138
19811 - Communication Agent Ingress Message Discarded 4-139
19814 - Communication Agent Peer has not responded to heartbeat 4-140
19816 - Communication Agent Connection State Changed 4-141
19817 - Communication Agent DB Responder detected a change in configurable control option parameter 4-141
19818 - Communication Agent DataEvent Mempool utilization 4-142
19820 - Communication Agent Routed Service Unavailable 4-142
19821 - Communication Agent Routed Service Degraded 4-143
19822 - Communication Agent Routed Service Congested 4-144
19823 - Communication Agent Routed Service Using Low-Priority Connection Group 4-145
19824 - Communication Agent Pending Transaction Utilization 4-146
19825 - Communication Agent Transaction Failure Rate 4-146
19826 - Communication Agent Connection Congested 4-147
19827 - SMS stack event queue utilization 4-148

19830 - Communication Agent Service Registration State Change 4-149
19831 - Communication Agent Service Operational State Changed 4-149
19832 - Communication Agent Reliable Transaction Failed 4-150
19833 - Communication Agent Service Egress Message Discarded 4-150
19842 - Communication Agent Resource-Provider Registered 4-151
19843 - Communication Agent Resource-Provider Resource State Changed 4-152
19844 - Communication Agent Resource-Provider Stale Status Received 4-152
19845 - Communication Agent Resource-Provider Deregistered 4-153
19846 - Communication Agent Resource Degraded 4-153
19847 - Communication Agent Resource Unavailable 4-154
19848 - Communication Agent Resource Error 4-154
19850 - Communication Agent Resource-User Registered 4-155
19851 - Communication Agent Resource-User Deregistered 4-155
19852 - Communication Agent Resource Routing State Changed 4-156
19853 - Communication Agent Resource Egress Message Discarded 4-156
19854 - Communication Agent Resource-Provider Tracking Table Audit Results 4-157
19855 - Communication Agent Resource Has Multiple Actives 4-158
19856 - Communication Agent Service Provider Registration State Changed 4-158
19857 - Communication Agent Service Provider Operational State Changed 4-159
19858 - Communication Agent Connection Rejected 4-159
19860 - Communication Agent Configuration Daemon Table Monitoring Failure 4-160
19861 - Communication Agent Configuration Daemon Script Failure 4-161
19862 - Communication Agent Ingress Stack Event Rate 4-162
19863 - Communication Agent Max Connections Limit In Connection Group Reached 4-162
19864 - ComAgent Successfully Set Host Server Hardware Profile 4-163
19865 - ComAgent Failed to Set Host Server Hardware Profile 4-163
19866 - Communication Agent Peer Group Status Changed 4-164
19867 - Communication Agent Peer Group Egress Message Discarded 4-164
19868 - Communication Agent Connection Rejected - Incompatible Network 4-165
19900 - Process CPU Utilization 4-166
19901 - CFG-DB Validation Error 4-166
19902 - CFG-DB Update Failure 4-167
19903 - CFG-DB post-update Error 4-167
19904 - CFG-DB Post-Update Failure 4-168
19905 - Measurement Initialization Failure 4-169
Diameter Signaling Router (DSR) Diagnostics (19910-19999) 4-169
19910 - Message Discarded at Test Connection 4-169
19911 - Test message discarded 4-170
Diameter Alarms and Events (8000-8299, 22000-22350, 22900-22999, 25600-25899) 4-170
8000 - MpEvFsmException 4-171
8001 - MpEvException 4-177
8002 - MpEvRxException 4-177
8003 - MpEvTxException 4-188

8004 - EvFsmAdState 4-192
8005 - EvFsmOpState 4-193
8006 - EvFsmException 4-194
8007 - EvException 4-202
8008 - EvRxException 4-203
8009 - EvTxException 4-211
8010 - MpIngressDrop 4-217
8011 - EcRate 4-217
8012 - MpRxNgnPsOfferedRate 4-218
8013 - MpNgnPsStateMismatch 4-218
8014 - MpNgnPsDrop 4-219
8015 - NgnPsMsgMisrouted 4-220
8016 - MpP16StateMismatch 4-220
8017 - MpTaskCpuCongested 4-221
8018 - P16MsgMisrouted 4-221
8019 - MpAnswerPriorityModeMismatch 4-222
8020 - MpRoutingThreadPoolStateMismatch 4-223
8100 - NormMsgMisrouted 4-223
8101 - DiagMsgMisrouted 4-224
8200 - MpRadiusMsgPoolCongested 4-224
8201 - RclRxTaskQueueCongested 4-225
8202 - RclItrPoolCongested 4-225
8203 - RclTxTaskQueueCongested 4-226
8204 - RclEtrPoolCongested 4-227
8205 - RadiusXactionFail 4-228
8206 - MpRxRadiusAllLen 4-228
8207 - MpRadiusKeyError 4-229
22001 - Message Decoding Failure 4-230
22002 - Peer Routing Rules with Same Priority 4-230
22004 - Maximum pending transactions allowed exceeded 4-231
22005 - No peer routing rule found 4-231
22007 - Inconsistent Application ID Lists from a Peer 4-232
22008 - Orphan Answer Response Received 4-233
22009 - Application Routing Rules with Same Priority 4-233
22010 - Specified DAS Route List not provisioned 4-234
22012 - Specified MCCS not provisioned 4-235
22013 - DAS Peer Number of Retransmits Exceeded for Copy 4-235
22014 - No DAS Route List specified 4-236
22016 - Peer Node Alarm Aggregation Threshold 4-237
22017 - Route List Alarm Aggregation Threshold 4-237
22018 - Maintenance Leader HA Notification to go Active 4-238
22019 - Maintenance Leader HA Notification to go OOS 4-239
22020 - Copy Message size exceeded the system configured size limit 4-239

22021 - Debug Routing Info AVP Enabled 4-240
22022 - Forwarding Loop Detected 4-240
22051 - Peer Unavailable 4-241
22052 - Peer Degraded 4-242
22053 - Route List Unavailable 4-243
22054 - Route List Degraded 4-244
22055 - Non-Preferred Route Group in Use 4-245
22056 - Connection Admin State Inconsistency Exists 4-246
22057 - ETG Rate Limit Degraded 4-247
22058 - ETG Pending Transaction Limit Degraded 4-247
22059 - Egress Throttle Group Message Rate Congestion Level changed 4-248
22060 - Egress Throttle Group Pending Transaction Limit Congestion Level changed 4-249
22061 - Egress Throttle Group Monitoring stopped 4-250
22062 - Actual Host Name cannot be determined for Topology Hiding 4-250
22063 - Diameter Max Message Size Limit Exceeded 4-251
22064 - Upon receiving Redirect Host Notification the Request has not been submitted for re-routing 4-251
22065 - Upon receiving Redirect Realm Notification the Request has not been submitted for re-routing 4-252
22066 - ETG-ETL Scope Inconsistency 4-253
22067 - ETL-ETG Invalid Association 4-253
22068 - TtpEvDoicException 4-254
22069 - TtpEvDoicOlr 4-257
22070 - TtpEvDegraded 4-258
22071 - TtgEvLossChg 4-259
22072 - TTP Degraded 4-260
22073 - TTP Throttling Stopped 4-260
22074 - TTP Maximum Loss Percentage Threshold Exceeded 4-261
22075 - Message is not routed to Application 4-262
22076 - TTG Maximum Loss Percentage Threshold Exceeded 4-262
22077 - Excessive Request Reroute Threshold Exceeded 4-263
22078 - Loop or Maximum Depth Exceeded in ART or PRT Search 4-264
22101 - Connection Unavailable 4-264
22102 - Connection Degraded 4-265
22103 - SCTP Connection Impaired 4-267
22104 - SCTP Peer is Operating with a Reduced IP Address Set 4-268
22105 - Connection Transmit Congestion 4-269
22106 - Ingress Message Discarded: DA-MP Ingress MessageRate Control 4-269
22200 - MP CPU Congested 4-270
22201 - MpRxAllRate 4-271
22202 - MpDiamMsgPoolCongested 4-272
22203 - PTR Buffer Pool Utilization 4-272
22204 - Request Message Queue Utilization 4-273

22205 - Answer Message Queue Utilization 4-274
22206 - Reroute Queue Utilization 4-275
22207 - DclTxTaskQueueCongested 4-276
22208 - DclTxConnQueueCongested 4-276
22209 - Message Copy Disabled 4-277
22214 - Message Copy Queue Utilization 4-278
22221 - Routing MPS Rate 4-278
22222 - Long Timeout PTR Buffer Pool Utilization 4-279
22223 - DA-MP Memory Utilization Threshold Crossed 4-280
22224 - Average Hold Time Limit Exceeded 4-281
22225 - Average Message Size Limit Exceeded 4-282
22328 - Connection is processing a higher than normal ingress messaging rate 4-283
22349 - IPFE Connection Alarm Aggregation Threshold 4-285
22350 - Fixed Connection Alarm Aggregation Threshold 4-286
22900 - DPI DB Table Monitoring Overrun 4-287
22901 - DPI DB Table Monitoring Error 4-287
22950 - Connection Status Inconsistency Exists 4-288
22960 - DA-MP Profile Not Assigned 4-288
22961 - Insufficient Memory for Feature Set 4-289
25607 - DSR Signaling Firewall is administratively Disabled 4-290
25608 - Abnormal DA-MP Firewall 4-290
25609 - Firewall Configuration Error encountered 4-291
25610 - DSR Signaling Firewall configuration inconsistency detected 4-291
25611 - ETG - Invalid DRMP Attributes 4-292
25612 - DSR ping failed 4-293
25805 - Invalid Shared TTG Reference 4-293
25806 - Invalid Internal SOAM Server Group Designation 4-294
Range Based Address Resolution (RBAR) Alarms and Events (22400-22424) 4-294
22400 - Message Decoding Failure 4-294
22401 - Unknown Application ID 4-295
22402 - Unknown Command Code 4-296
22403 - No Routing Entity Address AVPs 4-296
22404 - No valid Routing Entity Addresses found 4-297
22405 - Valid address received didn't match a provisioned address or address range 4-298
22406 - Routing attempt failed due to internal resource exhaustion 4-298
22407 - Routing attempt failed due to internal database inconsistency failure 4-299
Generic Application Alarms and Events (22500-22599) 4-299
22500 - DSR Application Unavailable 4-299
22501 - DSR Application Degraded 4-300
22502 - DSR Application Request Message Queue Utilization 4-301
22503 - DSR Application Answer Message Queue Utilization 4-302
22504 - DSR Application Ingress Message Rate 4-303
22520 - DSR Application Enabled 4-304

22521 - DSR Application Disabled 4-305
Full Address Based Resolution (FABR) Alarms and Events (22600-22640) 4-305
22600 - Message Decoding Failure 4-305
22601 - Unknown Application ID 4-306
22602 - Unknown Command Code 4-306
22603 - No Routing Entity Address AVPs 4-307
22604 - No Valid User Identity Addresses Found 4-308
22605 - No Destination address is found to match the valid User Identity address 4-308
22606 - Database or DB connection error 4-309
22607 - Routing attempt failed due to DRL queue exhaustion 4-310
22608 - Database query could not be sent due to DB congestion 4-310
22609 - Database connection exhausted 4-311
22610 - FABR DP Service congestion state change 4-311
22611 - FABR Blacklisted Subscriber 4-312
22631 - FABR DP Response Task Message Queue Utilization 4-312
22632 - ComAgent Registration Failure 4-313
Policy and Charging Application (PCA) Alarms and Events (22700-22799) 4-314
22700 - Protocol Error in Diameter Requests 4-314
22701 - Protocol Error in Diameter Answers 4-314
22702 - Database Hash Function Error 4-315
22703 - Diameter Message Routing Failure Due To Full DRL Queue 4-316
22704 - Communication Agent Error 4-316
22705 - SBR Error Response Received 4-317
22706 - Binding Key Not Found In Diameter Message 4-317
22707 - Diameter Message Processing Failure 4-318
22708 - PCA Function is Disabled 4-318
22709 - PCA Function is Unavailable 4-319
22710 - SBR Sessions Threshold Exceeded 4-320
22711 - SBR Database Error 4-321
22712 - SBR Communication Error 4-322
22713 - SBR Alternate Key Creation Error 4-322
22714 - SBR RAR Initiation Error 4-323
22715 - SBR Audit Suspended 4-323
22716 - SBR Audit Statistics Report 4-324
22717 - SBR Alternate Key Creation Failure Rate 4-324
22718 - Binding Not Found for Binding Dependent Session Initiate Request 4-325
22719 - Maximum Number of Sessions per Binding Exceeded 4-325
22720 - Policy SBR To PCA Response Queue Utilization Threshold Exceeded 4-326
22721 - Policy and Charging Server In Congestion 4-327
22722 - Policy Binding Sub-resource Unavailable 4-327
22723 - Policy and Charging Session Sub-resource Unavailable 4-329
22724 - Policy SBR Memory Utilization Threshold Exceeded 4-330
22725 - SBR Server In Congestion 4-330

22726 - SBR Queue Utilization Threshold Exceeded 4-331
22727 - SBR Initialization Failure 4-332
22728 - SBR Bindings Threshold Exceeded 4-332
22729 - PCRF Not Configured 4-333
22730 - Policy and Charging Configuration Error 4-334
22731 - Policy and Charging Database Inconsistency 4-335
22732 - SBR Process CPU Utilization Threshold Exceeded 4-335
22733 - SBR Failed to Free Binding Memory After PCRF Pooling Binding Migration 4-336
22734 - Policy and Charging Unexpected Stack Event Version 4-336
22735 - Policy DRA session initiation request received with no APN 4-337
22736 - SBR failed to free shared memory after a PCA function is disabled 4-338
22737 - Configuration Database Not Synced 4-338
22738 - SBR Database Reconfiguration State Transition 4-339
22740 - SBR Reconfiguration Plan Completion Failure 4-340
22741 - Failed to route PCA generated RAR 4-341
22742 - Enhanced Overload Control AdminState Mismatch 4-341
22743 - PCA Server Congested Due to Composite Resource Congestion 4-342
22750 - Enhanced Suspect Binding Removal Feature Enabled 4-342
22751 - Binding Audit Suppression by Suspect Binding Removal 4-343
Tekelec Virtual Operating Environment, TVOE (24400-24499) 4-344
24400 - TVOE libvirtd is down 4-344
24401 - TVOE libvirtd is hung 4-344
24402 - all TVOE libvirtd connections are in use 4-345
Computer Aided Policy Making, CAPM (25000-25499) 4-345
25000 - CAPM Update Failed 4-345
25001 - CAPM Action Failed 4-346
25002 - CAPM Exit Rule Template 4-347
25003 - CAPM Exit Trigger 4-347
25004 - Script failed to load 4-348
25005 - CAPM Generic Event 4-348
25006 - CAPM Generic Alarm - Minor 4-349
25007 - CAPM Generic Alarm - Major 4-349
25008 - CAPM Generic Alarm - Critical 4-350
OAM Alarm Management (25500-25899) 4-350
25500 - No DA-MP Leader Detected Alarm 4-350
25510 - Multiple DA-MP Leader Detected Alarm 4-351
25800 - Peer Discovery Failure 4-352
25801 - Peer Discovery Configuration Error Encountered 4-352
25802 - Realm Expiration Approaching 4-353
25803 - Peer Discovery - Inconsistent Remote Host Port Assignment 4-354
25804 - Peer Discovery State Change 4-354
Platform (31000-32800) 4-355
31000 - S/W fault 4-355

31001 - S/W status 4-355
31002 - Process watchdog failure 4-356
31003 - Tab thread watchdog failure 4-356
31100 - Database replication fault 4-357
31101 - Database replication to slave failure 4-358
31102 - Database replication from master failure 4-358
31103 - DB Replication update fault 4-359
31104 - DB Replication latency over threshold 4-360
31105 - Database merge fault 4-361
31106 - Database merge to parent failure 4-361
31107 - Database merge from child failure 4-362
31108 - Database merge latency over threshold 4-362
31109 - Topology config error 4-363
31110 - Database audit fault 4-364
31111 - Database merge audit in progress 4-364
31112 - DB replication update log transfer timed out 4-365
31113 - DB replication manually disabled 4-365
31114 - DB replication over SOAP has failed 4-366
31115 - Database service fault 4-366
31116 - Excessive shared memory 4-367
31117 - Low disk free 4-367
31118 - Database disk store fault 4-368
31119 - Database updatelog overrun 4-369
31120 - Database updatelog write fault 4-369
31121 - Low disk free early warning 4-370
31122 - Excessive shared memory early warning 4-370
31123 - Database replication audit command complete 4-371
31124 - ADIC error 4-371
31125 - Database durability degraded 4-372
31126 - Audit blocked 4-373
31127 - DB Replication Audit Complete 4-373
31128 - ADIC Found Error 4-374
31129 - ADIC Found Minor Issue 4-374
31130 - Network health warning 4-375
31131 - DB Ousted Throttle Behind 4-375
31132 - DB Replication Precedence Relaxed 4-376
31133 - DB Replication Switchover Exceeds Threshold 4-376
31134 - DB Site Replication To Slave Failure 4-377
31135 - DB Site Replication From Master Failure 4-377
31136 - DB Site Replication Precedence Relaxed 4-378
31137 - DB Site Replication Latency Over Threshold 4-378
31140 - Database perl fault 4-379
31145 - Database SQL fault 4-380

31146 - DB mastership fault 4-380
31147 - DB upsynclog overrun 4-381
31148 - DB lock error detected 4-381
31149 - DB Late Write Nonactive 4-382
31200 - Process management fault 4-383
31201 - Process not running 4-383
31202 - Unkillable zombie process 4-384
31206 - Process mgmt monitoring fault 4-384
31207 - Process resource monitoring fault 4-385
31208 - IP port server fault 4-385
31209 - Hostname lookup failed 4-386
31213 - Process scheduler fault 4-386
31214 - Scheduled process fault 4-387
31215 - Process resources exceeded 4-388
31216 - SysMetric configuration error 4-388
31217 - Network Health Warning 4-389
31220 - HA configuration monitor fault 4-389
31221 - HA alarm monitor fault 4-390
31222 - HA not configured 4-390
31223 - HA Heartbeat transmit failure 4-391
31224 - HA configuration error 4-391
31225 - HA service start failure 4-392
31226 - HA availability status degraded 4-392
31227 - HA availability status failed 4-393
31228 - HA standby offline 4-394
31229 - HA score changed 4-394
31230 - Recent alarm processing fault 4-395
31231 - Platform alarm agent fault 4-396
31232 - Late heartbeat warning 4-396
31233 - HA Path Down 4-397
31234 - Untrusted Time Upon Initialization 4-397
31235 - Untrusted Time After Initialization 4-398
31236 - HA Link Down 4-399
31240 - Measurements collection fault 4-399
31250 - RE port mapping fault 4-400
31260 - SNMP Agent 4-400
31261 - SNMP Configuration Error 4-401
31270 - Logging output 4-401
31280 - HA Active to Standby transition 4-402
31281 - HA Standby to Active transition 4-403
31282 - HA Management Fault 4-403
31283 - Lost Communication with server 4-404
31284 - HA Remote Subscriber Heartbeat Warning 4-404

31285 - HA Node Join Recovery Entry 4-405
31286 - HA Node Join Recovery Plan 4-405
31287 - HA Node Join Recovery Complete 4-406
31288 - HA Site Configuration Error 4-406
31290 - HA Process Status 4-407
31291 - HA Election Status 4-407
31292 - HA Policy Status 4-408
31293 - HA Resource Link Status 4-408
31294 - HA Resource Status 4-409
31295 - HA Action Status 4-410
31296 - HA Monitor Status 4-410
31297 - HA Resource Agent Info 4-411
31298 - HA Resource Agent Detail 4-411
31299 - HA Notification Status 4-412
31300 - HA Control Status 4-412
31301 - HA Topology Events 4-413
31322 - HA Configuration Error 4-413
32100 - Breaker Panel Feed Unavailable 4-414
32101 - Breaker Panel Breaker Failure 4-414
32102 - Breaker Panel Monitoring Failure 4-415
32103 - Power Feed Unavailable 4-415
32104 - Power Supply 1 Failure 4-416
32105 - Power Supply 2 Failure 4-416
32106 - Power Supply 3 Failure 4-417
32107 - Raid Feed Unavailable 4-417
32108 - Raid Power 1 Failure 4-418
32109 - Raid Power 2 Failure 4-418
32110 - Raid Power 3 Failure 4-419
32111 - Device Failure 4-419
32112 - Device Interface Failure 4-420
32113 - Uncorrectable ECC memory error 4-420
32114 - SNMP get failure 4-421
32115 - TPD NTP Daemon Not Synchronized Failure 4-422
32116 - TPD Server's Time Has Gone Backwards 4-423
32117 - TPD NTP Offset Check Failure 4-424
32300 - Server fan failure 4-426
32301 - Server internal disk error 4-426
32302 - Server RAID disk error 4-427
32303 - Server Platform error 4-428
32304 - Server file system error 4-428
32305 - Server Platform process error 4-429
32306 - Server RAM shortage error 4-430
32307 - Server swap space shortage failure 4-430

32308 - Server provisioning network error 4-431
32309 - Eagle Network A Error 4-432
32310 - Eagle Network B Error 4-433
32311 - Sync Network Error 4-433
32312 - Server disk space shortage error 4-434
32313 - Server default route network error 4-435
32314 - Server temperature error 4-436
32315 - Server mainboard voltage error 4-437
32316 - Server power feed error 4-437
32317 - Server disk health test error 4-438
32318 - Server disk unavailable error 4-439
32319 - Device error 4-440
32320 - Device interface error 4-440
32321 - Correctable ECC memory error 4-441
32322 - Power Supply A error 4-442
32323 - Power Supply B error 4-443
32324 - Breaker panel feed error 4-443
32325 - Breaker panel breaker error 4-444
32326 - Breaker panel monitoring error 4-447
32327 - Server HA Keepalive error 4-448
32328 - DRBD is unavailable 4-449
32329 - DRBD is not replicating 4-450
32330 - DRBD peer problem 4-450
32331 - HP disk problem 4-451
32332 - HP Smart Array controller problem 4-452
32333 - HP hpacucliStatus utility problem 4-452
32334 - Multipath device access link problem 4-453
32335 - Switch link down error 4-454
32336 - Half Open Socket Limit 4-454
32337 - Flash Program Failure 4-455
32338 - Serial Mezzanine Unseated 4-456
32339 - TPD Max Number Of Running Processes Error 4-456
32340 - TPD NTP Daemon Not Synchronized Error 4-457
32341 - TPD NTP Daemon Not Synchronized Error 4-458
32342 - NTP Offset Check Error 4-459
32343 - TPD RAID disk 4-460
32344 - TPD RAID controller problem 4-461
32345 - Server Upgrade snapshot(s) invalid 4-462
32346 - OEM hardware management service reports an error 4-462
32347 - The hwmgmtcliStatus daemon needs intervention 4-463
32348 - FIPS subsystem problem 4-464
32349 - File Tampering 4-464
32350 - Security Process Terminated 4-465

32500 - Server disk space shortage warning 4-466
32501 - Server application process error 4-466
32502 - Server hardware configuration error 4-467
32503 - Server RAM shortage warning 4-468
32504 - Software Configuration Error 4-468
32505 - Server swap space shortage warning 4-469
32506 - Server default router not defined 4-470
32507 - Server temperature warning 4-471
32508 - Server core file detected 4-472
32509 - Server NTP Daemon not synchronized 4-473
32510 - CMOS battery voltage low 4-474
32511 - Server disk self test warning 4-474
32512 - Device warning 4-475
32513 - Device interface warning 4-476
32514 - Server reboot watchdog initiated 4-476
32515 - Server HA failover inhibited 4-477
32516 - Server HA Active to Standby transition 4-477
32517 - Server HA Standby to Active transition 4-478
32518 - Platform Health Check failure 4-479
32519 - NTP Offset Check failure 4-479
32520 - NTP Stratum Check failure 4-480
32521 - SAS Presence Sensor Missing 4-481
32522 - SAS Drive Missing 4-482
32523 - DRBD failover busy 4-483
32524 - HP disk resync 4-483
32525 - Telco Fan Warning 4-484
32526 - Telco Temperature Warning 4-485
32527 - Telco Power Supply Warning 4-485
32528 - Invalid BIOS value 4-486
32529 - Server Kernel Dump File Detected 4-487
32530 - TPD Upgrade Failed 4-487
32531 - Half Open Socket Warning Limit 4-488
32532 - Server Upgrade Pending Accept/Reject 4-488
32533 - TPD Max Number Of Running Processes Warning 4-489
32534 - TPD NTP Source Is Bad Warning 4-490
32535 - TPD RAID disk resync 4-491
32536 - TPD Server Upgrade snapshot(s) warning 4-491
32537 - FIPS subsystem warning event 4-492
32538 - Platform Data Collection Error 4-493
32539 - Server Patch Pending Accept/Reject 4-493
32540 - CPU Power limit mismatch 4-494
32700 - Telco Switch Notification 4-494
32701 - HIDS Initialized 4-495

32702 - HIDS Baseline Deleted 4-495
32703 - HIDS Enabled 4-495
32704 - HIDS Disabled 4-496
32705 - HIDS Monitoring Suspended 4-496
32706 - HIDS Monitoring Resumed 4-496
32707 - HIDS Baseline Updated 4-497
DM-IWF (33000-33024) 4-497
33000 - MAP-to-Diameter Service Registration Failure on DA-MP 4-497
33001 - Diameter-to-MAP Service Registration Failure on DA-MP 4-498
33002 - DM-IWF DA-MP not associated with a Place 4-498
33003 - Insufficient memory for DM-IWF 4-499
33004 - DM-IWF Transaction Response Queue Utilization 4-500
33005 - DM-IWF PTR Pool Utilization 4-500
33006 - MD-IWF Service Congestion 4-501
33007 - MD-IWF Error 4-502
33008 - DM-IWF maximum pending transactions allowed exceeded 4-502
33009 - DM-IWF unexpected Answer response received from a SS7-MP 4-503
33010 - MD-IWF ComAgent Connection exhausted 4-504
33011 - DM-IWF Answer Timeout 4-504
33012 - DM-IWF encode decode error 4-505
33013 - DRL queue exhaustion 4-505
33014 - Incompatible DA-MP Profile for DM-IWF 4-506
33015 - DM-IWF Diameter message size exceeded maximum supported size 4-507
MD-IWF (33050-33099) 4-507
33050 - MD-IWF Ingress Message Rate 4-507
33051 - MD-IWF Application Degraded or Unavailable 4-508
33052 - MD-IWF Notified that DM-IWF Service Status is Down 4-509
33053 - MD-IWF DiamTrans Task Queue Utilization 4-510
33054 - MD-IWF MapTrans Task Queue Utilization 4-510
33055 - MD-IWF DAMPInterface Task Queue Utilization 4-511
33056 - MD-IWF ComAgent Provider Registration Failure on SS7-MP 4-512
33057 - MD-IWF ComAgent User Registration Failure on SS7-MP 4-512
33058 - MD-IWF DiamToMap PTR Utilization 4-513
33059 - MD-IWF MapToDiam PTR Utilization 4-513
33060 - SS7-MP Profile Not Assigned 4-514
33062 - Insufficient Memory for MD-IWF 4-515
33063 - MD-IWF SS7-MP not associated with a Place 4-515
33065 - MD-IWF Resource Exhaustion 4-516
33066 - MD-IWF orphan Diameter Answer message received 4-517
33067 - MD-IWF orphan MAP Response message received 4-517
33068 - MD-IWF MAP Response timeout 4-518
33069 - MD-IWF Diameter Answer timeout 4-518
33070 - MD-IWF Generated Diameter Answer error message due to Diameter Exception 4-519

33071 - MD-IWF Generated MAP Error Response due to MAP exception 4-520
33072 - MD-IWF received TCAP Notice from SS7 network 4-520
33073 - MD-IWF admin state set to Enabled 4-521
33074 - MD-IWF admin state set to Disabled 4-521
33075 - MD-IWF received ComAgent error or DM-IWF NACK 4-522
33076 - MD-IWF received Diameter Anwer from unexpected DA-MP 4-522
33077 - MD-IWF address translation failed 4-523
33078 - MD-IWF received Diameter EIR message but Destination-Host AVP not present or not found in mapping table 4-523
33079 - MD-IWF message translation failed 4-524
33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message . 4-524
GLA (33100-33149) 4-525
33100 - GLA Message Decoding Failure 4-525
33101 - GLA Incorrect Application ID or Command Code 4-526
33102 - GLA Missing Subscriber ID 4-527
33103 - GLA Communication Agent Error 4-527
33104 - GLA Duplicate Subscriber ID 4-528
33105 - Routing Attempt failed due to queue exhaustion 4-528
33106 - GLA Communication Agent Timeout 4-529
33120 - Policy SBR Binding Sub-Resource Unavailable 4-530
33121 - GLA pSBR-B Response Task Message Queue Utilization 4-530
Diameter Custom Applications (DCA) Framework Alarms and Events (33300-33630) 4-531
33300 - Create Application Version Failure 4-531
33301 - Update Config Data Failure 4-532
33302 - Delete Application Version Failure 4-532
33303 - U-SBR Event Queue Utilization 4-533
33304 - DCA Runtime Errors 4-534
33305 - DCA Procedure Not Found 4-534
33306 - U-SBR Resolution Failure 4-535
33307 - Diameter Message Routing Failure Due To Full DRL Queue 4-536
33308 - DCA to U-SBR ComAgent Error 4-536
33309 - DCA Script Compilation Error 4-537
33310 - U-SBR Sub-resource Unavailable 4-537
33311 - DCA Application Reloaded 4-538
33312 - DCA Script Generation Error 4-538
33313 - DCA U-SBR Logical Name Mismatch 4-539
33314 - Custom MEAL differentiation error 4-540
DCA Custom MEAL Event Templates 4-540
Independent SBR Alarms and Events (12003-12010, 33730-33830) 4-541
12003 - SBR Congestion State 4-541
12007 - SBR Active Sess Binding Threshold 4-542
12010 - SBR Proc Term 4-542
33730 - U-SBR Database Audit Statistics Report 4-543

vSTP Alarms and Events (70000-70999) 4-544
70000 - Association Down 4-544
70001 - Link Down 4-544
70002 - RSP/Destination Unavailable 4-545
70003 - RSP/Destination Route Unavailable 4-546
70004 - Linkset Unavailable 4-547
70005 - Link Unavailable 4-547
70006 - Preferred Route Unavailable 4-548
70007 - Node isolated - All links down 4-549
70008 - Linkset Restricted 4-549
70009 - Link Congested 4-550
70050 - SCTP connection refused 4-551
70051 - Failed to configure Transport 4-551
70052 - Far-end closed the connection 4-552
70053 - SCTP connection closed 4-552
70054 - Remote IP Address state change 4-553
70055 - Association admin state change 4-554
70056 - Link admin state change 4-554
70057 - Received invalid M3UA message 4-555
70058 - Received M3UA ERROR 4-556
70059 - Failed to send DATA message 4-557
70101 - Transmission Association Queue Congestion Crossed 4-558
70102 - MTP3 Ingress Link MSU TPS Crossed 4-558
70103 - MTP3 Egress Link MSU TPS Crossed 4-559
70104 - MTP3 Ingress Link Management TPS Crossed 4-559
70105 - Transmission Association Queue Discard Crossed 4-560
70107 - vSTP SCCP Stack Event Queue Utilization 4-561
70108 - vSTP M3RL Stack Event Queue Utilization 4-561
70109 - vSTP M3RL Network Management Event Queue Utilization 4-562
70110 - vSTP M3UA Stack Event Queue Utilization 4-562
70111 - vSTP M2PA Stack Event Queue Utilization 4-563
70112 - vSTP M3UA Tx Stack Event Queue Utilization 4-564
70201 - M2PA link operational state changed 4-564
70202 - M2PA link failed 4-565
70203 - M2PA Ingress message discarded 4-565
70204 - M2PA Egress message discarded 4-566
70205 - M2PA Message Encoding Failed 4-566
70206 - M2PA Message Decoding Failed 4-567
70271 - SCCP Received Invalid Message 4-567
70272 - SCCP Message Translation Failed 4-568
70273 - SCCP Message Routing Failed 4-568
70274 - SGMG Message Invalid 4-569
70275 - GTT SCCP Loop Detected 4-569

70276 - GTT Load Sharing Failed 4-570

5 Key Performance Indicators (KPIs)

General KPIs information 5-1
KPIs overview 5-1
KPIs 5-1
KPIs server elements 5-1
Viewing KPIs 5-2
KPIs data export elements 5-2
Exporting KPIs 5-3
Computer Aided Policy Making (CAPM) KPIs 5-4
Communication Agent (ComAgent) KPIs 5-5
Diameter (DIAM) KPIs 5-5
DM-IWF KPIs 5-5
DP KPIs 5-6
GLA KPIs 5-7
IDIH KPIs 5-7
IP Front End (IPFE) KPIs 5-7
MD-IWF KPIs 5-8
Message Processor (MP) KPIs 5-8
Full Address Based Resolution (FABR) KPIs 5-9
Platform KPIs 5-9
Policy and Charging Application (PCA) KPIs 5-10
Process-based KPIs 5-10
Provisioning KPIs 5-11
Range Based Address Resolution (RBAR) KPIs 5-13
Subscriber Binding Repository (SBR) KPIs 5-13
SS7/Sigtran KPIs 5-14
DCA Framework KPIs 5-15
DCA Custom MEAL KPIs 5-15
U-SBR KPIs 5-16

List of Figures

2-1 Oracle System Login 2-12
2-2 Paginated Table 2-15
2-3 Scrollable Table 2-15
2-4 Form Page 2-16
2-5 Tabbed Pages 2-16
2-6 Tabbed Pages 2-16
2-7 Report Output 2-17
2-8 Sorting a Table by Column Header 2-17
2-9 Clear Field Control X 2-18
2-10 Optional Layout Element Toolbar 2-19
2-11 Automatic Error Notification 2-19
2-12 Examples of Filter Styles 2-20
3-1 Flow of Alarms 3-2
3-2 Alarm Indicators Legend 3-3
3-3 Trap Count Indicator Legend 3-3
4-1 Breaker Panel LEDs 4-445
4-2 Breaker Panel Setting 4-446

List of Tables

1-1 Admonishments ... 1-2
2-1 User Interface Elements ... 2-3
2-2 Main Menu Options ... 2-6
2-3 Main Menu Icons ... 2-13
2-4 Example Action Buttons ... 2-18
2-5 Submit Buttons ... 2-18
2-6 Filter Control Elements ... 2-20
3-1 Alarm/Event ID Ranges ... 3-4
3-2 Alarm and Event Types ... 3-5
3-3 Schedule Active Alarm Data Export Elements ... 3-7
3-4 Schedule Event Data Export Elements ... 3-10
3-5 Data Export Elements ... 3-14
3-6 Active Tasks Elements ... 3-17
3-7 Active Tasks Report Elements ... 3-19
3-8 Scheduled Tasks Elements ... 3-21
5-1 KPIs Server Elements ... 5-1
5-2 Schedule KPI Data Export Elements ... 5-2
5-3 CAPM KPIs ... 5-4
5-4 Communication Agent KPIs ... 5-5
5-5 DIAM KPIs ... 5-5
5-6 DM-IWF KPIs ... 5-5
5-7 DP KPIs ... 5-6
5-8 IPFE KPIs ... 5-7
5-9 MP KPIs ... 5-8
5-10 FABR KPIs ... 5-9
5-11 Platform KPIs ... 5-9
5-12 PCA KPIs ... 5-10
5-13 Process-based KPIs ... 5-10
5-14 Provisioning KPIs ... 5-11
5-15 RBAR KPIs ... 5-13
5-16 SBR KPIs ... 5-13
5-17 SBR-Binding KPIs ... 5-14
5-18 SBR-Session KPIs ... 5-14
5-19 SS7/Sigtran KPIs ... 5-14

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
June 2016	• New alarms and events added for new features, DCA, U-SBR, I-SBR, and COMCOL. • KPIs added for DCA and U-SBR.

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.

- 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 provides lists of 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, and Locate Product Documentation on the Customer Support Site.
- User Interface Introduction provides basic information about the DSR user interface.
- 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.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of personal injury.)
	Warning: (This icon and text indicate the possibility of equipment damage.)
	Caution: (This icon and text indicate the possibility of service interruption.)

Locate Product Documentation on the Oracle Help Center Site

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

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

The Communications Documentation page displays. Most products covered by these documentation sets display under the headings Network Session Delivery and Control Infrastructure and Platforms.

4. Click on your product and then the release number.

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

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

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training at http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site at www.oracle.com/education/contacts

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.

Emergency Response

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

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective

action. Critical situations affect service and/or system operation resulting in one or several of these situations:

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

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

2

User Interface Introduction

This section describes the organization and usage of the application's user interface. In it you can find information about how the interface options are organized, how to use widgets and buttons, and how filtering and other page display options work.

User Interface Organization

The user interface is the central point of user interaction within an application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to an application and its functions.

The core framework presents a common set of Main Menu options that serve various applications. The common Main Menu options are:

- Administration
- Configuration
- Alarms and Events
- Security Log
- Status and Manage
- Measurements
- Help
- Legal Notices
- Logout

Applications build upon this framework to present features and functions. Depending on your application, some or all of the following Main Menu options may display on the Network Operation, Administration, and Maintenance (**NOAM**) GUI:

- Communication Agent
- Diameter Common
- Diameter
- **UDR** (User Data Repository)
- MAP-Diameter IWF
- **RADIUS** (Remote Authentication Dial-In User Service)
- **SBR** (Session Binding Repository)

- Policy and Charging
- **DCA** (DOIC Capabilities Announcement) Framework

The DSR System OAM GUI may present even more Main Menu options as listed below. The end result is a flexible menu structure that changes according to the application needs and features activated.

- Transport Manager
- SS7/Sigtran
- RBAR (Range Based Address Resolution)
- FABR (Full Address Based Resolution)
- **GLA** (Gateway Location Application)
- MAP-Diameter IWF
- RADIUS
- SBR
- Mediation
- Policy and Charging
- DCA Framework
- IPFE (IP Front End)

Note that the System OAM (SOAM) Main Menu options differ from the Network OAM (NOAM) options. Some Main Menu options are configurable from the NOAM server and view-only from the SOAM (**SOAM**) server. This remains true for other applications.

User Interface Elements

Table 2-1 describes elements of the user interface.

Table 2-1 User Interface Elements

Element	Location	Function
Identification Banner	Top bar across the web page	The left side of the banner provides the following information: • Displays the company name, • product name and version, and • the alarm panel. The right side of the banner: • Allows you to pause any software updates. • Links to the online help for all software. • Shows the user name of the currently logged-in user. • Provides a link to log out of the GUI.
Main Menu	Left side of screen, under banners	A tree-structured menu of all operations that can be performed through the user interface. The plus character (+) indicates a menu item contains subfolders. • To display submenu items, click the plus character, the folder, or anywhere on the same line. • To select a menu item that does not have submenu items, click on the menu item text or its associated symbol.

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
Work Area	Right side of panel under status	Consists of three sections: Page Title Area, Page Control Area (optional), and Page Area. • Page Title Area: Occupies the top of the work area. It displays the title of the current page being displayed, date and time, and includes a link to context-sensitive help. • Page Control Area: Located below the Page Title Area, this area shows controls for the Page Area (this area is optional). When available as an option, filter controls display in this area. The Page Control Area contains the optional layout element toolbar, which displays different elements depending on which GUI page is selected. For more information, see Optional Layout Element Toolbar. • Page Area: Occupies the bottom of the work area. This area is used for all types of operations. It displays all options, status, data, file, and query screens. Information or error messages are displayed in a message box at the top of this section. A horizontal and/or vertical scroll bar is provided when the displayed information exceeds the page area of the screen. When a user first logs in, this area displays the application

Table 2-1 (Cont.) User Interface Elements

Element	Location	Function
		user interface page. The page displays a user-defined welcome message. To customize the message, see Customizing the Login Message.
Session Banner	Across the bottom of the web page	The left side of the banner provides the following session information: • The name of the machine to which the user is connected, and whether the user is connected via the VIP or directly to the machine. • The **HA** state of the machine to which the user is connected. • The role of the machine to which the user is connected. The right side of the banner shows the alarm panel.

Main Menu Options

Table 2-2 describes all main menu user interface options.

Note: The menu options can differ according to the permissions assigned to a user's login account. For example, the Administration menu options do not display on the screen of a user who does not have administrative privileges.

Note: Some menu items are configurable only on the Network OAM and view-only on the System OAM; and some menu options are configurable only on the System OAM.

Note: Some features do not display in the main menu until the features are activated.

Table 2-2 Main Menu Options

Menu Item	Function
Administration	The Administration menu allows the user to: • General Options. Configure options such as password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Set up and manage user accounts • Configure group permissions • View session information • Manage sign-on certificates • Authorize IP addresses to access the user interface • Configure **SFTP** user information • View the software versions report • Upgrade management including backup and reporting • Authenticate **LDAP** servers • Configure **SNMP** trapping services • Configure an export server • Configure **DNS** elements
Configuration	On the NOAM, allows the user to configure: • Network Elements • Network Devices • Network Routes • Services • Servers • Server Groups • Resource Domains • Places • Place Associations • Interface and Port **DSCP**
Alarms and Events	Allows the user to view: • Active alarms and events • Alarm and event history • Trap log
Security Log	Allows the user to view, export, and generate reports from security log history.
Status and Manage	Allows the user to monitor the individual and collective status of Network Elements, Servers, HA functions, Databases, **KPI**s, system Processes, and Tasks. The user can perform actions required for server maintenance, database management, data, and ISO file management.
Measurements	Allows the user to view and export measurement data.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
Transport Manager (optional)	On the SOAM, allows the user to configure adjacent nodes, configuration sets, or transports. A maintenance option allows the user to perform enable, disable, and block actions on the transport entries. This option only displays with the DSR application.
Communication Agent (optional)	Allows the user to configure Remote Servers, Connection Groups, and Routed Services. The user can perform actions to enable, disable, and block connections. Also allows the user to monitor the status of Connections, Routed Services, and **HA** Services.
SS7/Sigtran (optional)	On the SOAM, allows the user to configure various users, groups, remote signaling points, links, and other items associated with SS7/Sigtran; perform maintenance and troubleshooting activities; and provides a command line interface for bulk loading SS7 configuration data. This option only displays with the DSR application.
Diameter Common (optional)	Allows the user to view or configure: • Dashboard, configure on the NOAM; view on both OAMs • Network Identifiers on the SOAM - MCC Ranges • Network Identifiers on the NOAM - **MCCMNC** and MCCMNC Mapping • MPs (on the SOAM) - editable Profile parameters and Profile Assignments The DSR Bulk Import and Export functions are available on both OAMs for the data configured on that OAM.
Diameter (optional)	Allows the user to configure, modify, and monitor Diameter routing: • On the NOAMP, Diameter Topology Hiding and Egress Throttle List configuration • On the SOAM, Diameter Configuration, Maintenance, Reports, Troubleshooting with **IDIH**, **AVP** Dictionary, and Diameter Mediation configuration
UDR (User Data Repository) (optional)	Allows the user to add, edit, store, and manage subscriber and pool data. The user can also monitor the import, export, and subscribing client status. This option only displays with the UDR application.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
RBAR (Range-Based Address Resolution) (optional)	Allows the user to configure the following Range-Based Address Resolution (RBAR) settings: • Applications • Exceptions • Destinations • Address Tables • Addresses • Address Resolutions • System Options This is accessible from the SOAM only. This option only displays with the DSR application.
FABR (Full Address Based Resolution) (optional)	Allows the user to configure the following Full Address Based Resolution (FABR) settings: • Applications • Exceptions • Default Destinations • Address Resolutions • System Options This is accessible from the SOAM only. This option is only available with the DSR application.
Gateway Location Application (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • Exceptions • Options GLA can deploy with Policy DRA (in the same DA-MP or a separate DA-MP). This option only displays with the DSR application.
MAP-Diameter Interworking (optional)	On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for the DM-IWF DSR Application: • DM-IWF Options • Diameter Exception On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for the MD-IWF **SS7** Application: • **MD-IWF** Options • Diameter Realm • Diameter Identity **GTA** • GTA Range to PC • **MAP** Exception • **CCNDC** Mapping This option only displays with the DSR application.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
RADIUS (Remote Authentication Dial-In User Service) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • Network Options • Message Authenticator Configuration Sets • Shared Secret Configuration Sets • Ingress Status Server Configuration Sets • Message Conversion Configuration Sets • **NAS** Node This option only displays with the DSR application.
SBR (Session Binding Repository) (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for: • **SBR** Databases • SBR Database Resizing Plans • SBR Data Migration Plans • Database Options Additionally, on the NOAMP, users are allowed to perform maintenance tasks, edit options, and view elements for: • Maintenance – SBR Database Status – SBR Status – SBR Database Reconfiguration Status This option only displays with the DSR application.
Mediation	Allows the user to make routable decisions to end the reply, drop the message, or set the destination realm.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
Policy and Charging (optional)	On the NOAMP, allows the user to perform configuration tasks, edit options, and view elements for: • General Options • Access Point Names • Policy DRA – PCRF Pools – PCRF Sub-Pool Selection Rules – Network-Wide Options • Online Charging DRA – OCS Session State – Realms – Network-Wide Options • Alarm Settings • Congestion Options Additionally on the **NOAMP**, users are allowed to perform maintenance tasks, edit options, and view elements for: • Maintenance – SBR Database Status – SBR Status – SBR Database Reconfiguration Status – Policy Database Query On the SOAM, allows the user to perform configuration tasks, edit options, and view elements for: • General Options • Access Point Names • Policy DRA – PCRFs – Binding Key Priority – **PCRF** Pools – PCRF Pool to **PRT** Mapping – PCRF Sub-Pool Selection Rules – Policy Clients – Suspect Binding Removal Rules – Site Options • Online Charging **DRA** – OCSs – **CTF**s – **OCS** Session State – Realms • Error Codes • Alarm Settings • Congestion Options This option only displays with the DSR application.

Table 2-2 (Cont.) Main Menu Options

Menu Item	Function
DCA Framework (optional)	Allows the user to perform configuration tasks, edit system options, and view elements for DCA applications: • Custom **MEAL**s (Measurements, Events, Alarms, and Logs) • General Options • Trial **MP**s assignment • Application Control • System Options
IPFE (optional)	Allows the user to configure IP Front End (IPFE) options and **IP** List **TSA**s. This is accessible from the SOAM server only. This option only displays with the DSR application.
Help	Launches the Help system for the user interface
Legal Notices	Product Disclaimers and Notices
Logout	Allows the user to log out of the user interface

Missing Main Menu options

Permissions determine which Main Menu options are visible to users. Permissions are defined through the Group Administration page. The default group, admin, is permitted access to all GUI options and functionality. Additionally, members of the admin group set permissions for other users.

Main Menu options vary according to the group permissions assigned to a user's account. Depending on your user permissions, some menu options may be missing from the Main Menu. For example, Administration menu options do not display on your screen if you do not have administrative permissions. For more information about user permissions, see *Group Administration* in the OAM section of the online help, or contact your system administrator.

Common Graphical User Interface Widgets

Common controls allow you to easily navigate through the system. The location of the controls remains static for all pages that use the controls. For example, after you become familiar with the location of the display filter, you no longer need to search for the control on subsequent pages because the location is static.

Supported Browsers

This application supports the use of Microsoft® Internet Explorer 8.0, 9.0, or 10.0.

is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details

System Login Page

Access to the user interface begins at the System Login page. The System Login page allows users to log in with a username and password and provides the option of changing the password upon login. The System Login page also features a date and time stamp reflecting the time the page was last refreshed. Additionally, a customizable login message displays just below the **Log In** button.

The user interface is accessed via HTTPS, a secure form of the HTTP protocol. When accessing a server for the first time, HTTPS examines a web certificate to verify the identity of the server. The configuration of the user interface uses a self-signed web certificate to verify the identity of the server. When the server is first accessed, the supported browser warns the user that the server is using a self-signed certificate. The browser requests confirmation that the server can be trusted. The user is required to confirm the browser request to gain access.

Customizing the Login Message

Before logging in, the System Login page displays. You can create a login message that displays just below the **Log In** button on the System Login page.

Figure 2-1 Oracle System Login

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Locate **LoginMessage** in the **Variable** column.
3. Enter the login message text in the **Value** column.

4. Click **OK** or **Apply** to submit the information.

   A status message displays at the top of the Configuration Administration page to inform you if the operation was successful.

The next time you log into the user interface, the login message text displays.

Accessing the DSR Graphical User Interface

In DSR, some configuration is done at the **NOAM** server, while some is done at the **SOAM** server. Because of this, you need to access the DSR graphical user interface (GUI) from two servers. Certificate Management (Single Sign-On) can be configured to simplify accessing the DSR GUI on the NOAM and the SOAM.

For information on configuring Single Sign-On certificates, see **OAM** > **Administration** > **Access Control** > **Certificate Management** in the DSR online help.

After the certificates have been configured, you can log into the DSR GUI on any NOAM or SOAM, and access the DSR GUI on other servers (NOAM or other SOAMs) without having to re-enter your login credentials.

1. In the browser URL field, enter the fully qualified hostname of the NOAM server, for example https://dsr-no.yourcompany.com.

   When using Single Sign-On, you cannot use the IP address of the server.

2. When prompted by the browser, confirm that the server can be trusted.

   The System Login page displays.

3. Enter the Username and Password for your account.

   The DSR GUI for the NOAM displays.

4. To access the DSR GUI for the SOAM, open another browser window and enter the fully qualified hostname of the SOAM.

   The DSR GUI for the SOAM displays.

You can toggle between the DSR GUI on the NOAM and the DSR GUI on the SOAM as you perform configuration tasks.

Main Menu Icons

This table describes the icons used in the Main Menu.

Table 2-3 Main Menu Icons

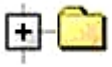
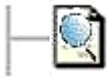
Icon	Name	Description
	Folder	Contains a group of operations. If the folder is expanded by clicking the plus (+) sign, all available operations and sub-folders are displayed. Clicking the minus (-) collapses the folder.

Table 2-3 (Cont.) Main Menu Icons

Icon	Name	Description
	Config File	Contains operations in an Options page.
	File with Magnifying Glass	Contains operations in a Status View page.
	File	Contains operations in a Data View page.
	Multiple Files	Contains operations in a File View page.
	File with Question Mark	Contains operations in a Query page.
	User	Contains operations related to users.
	Group	Contains operations related to groups.
	Task	Contains operations related to Tasks
	Help	Launches the Online Help.
	Logout	Logs the user out of the user interface.

Work Area Displays

In the user interface, tables, forms, tabbed pages, and reports are the most common formats.

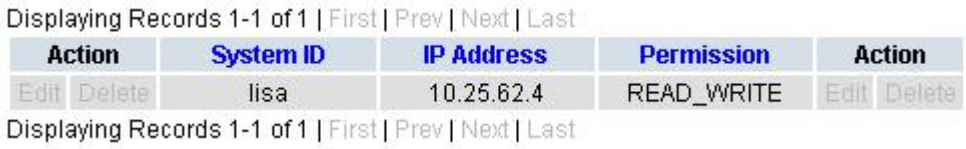
Note: Screen shots are provided for reference only and may not exactly match a specific application's GUI.

Tables

Paginated tables describe the total number of records being displayed at the beginning and end of the table. They provide optional pagination with **First | Prev | Next | Last** links at both the beginning and end of this table type. Paginated tables also contain

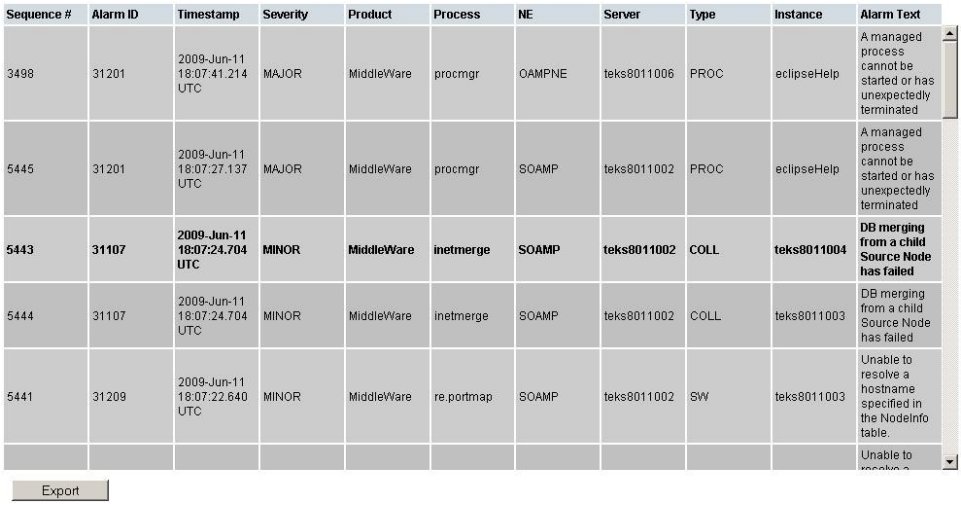
action links on the beginning and end of each row. For more information on action links and other page controls, see Page Controls.

Figure 2-2 Paginated Table



Scrollable tables display all of the records on a single page. The scroll bar, located on the right side of the table, allows you to view all records in the table. Scrollable tables also provide action buttons that operate on selected rows. For more information on buttons and other page controls, see Page Controls.

Figure 2-3 Scrollable Table

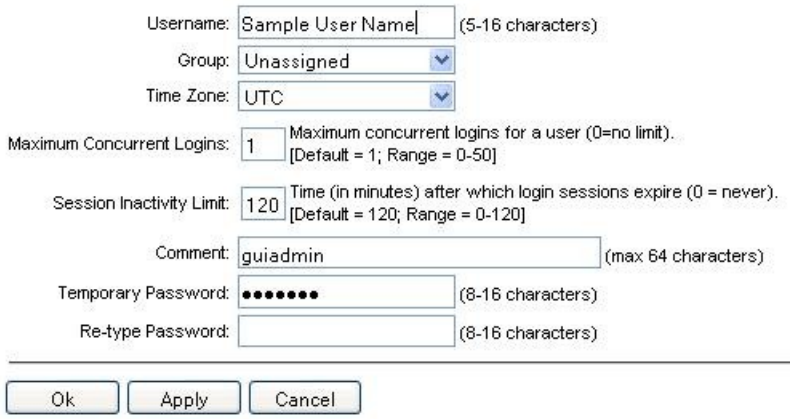


Note: Multiple rows can be selected in a scrollable table. Add rows one at a time using CTRL-click. Add a span of rows using SHIFT-click.

Forms

Forms are pages on which data can be entered. Forms are typically used for configuration. Forms contain fields and may also contain a combination of lists, buttons, and links.

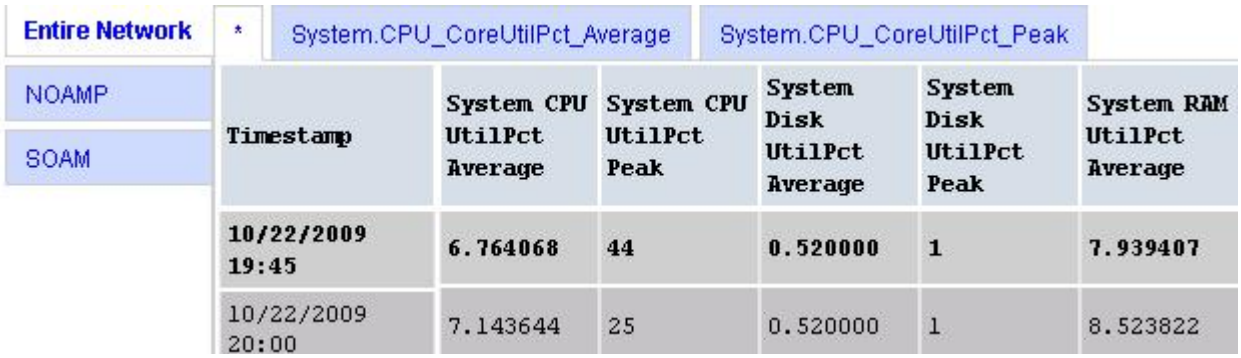
Figure 2-4 Form Page



Tabbed pages

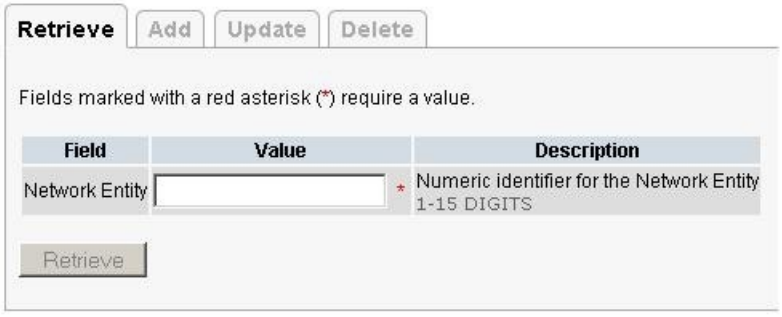
Tabbed pages provide collections of data in selectable tabs. Click on a tab to see the relevant data on that tab. Tabbed pages also group Retrieve, Add, Update, and Delete options on one page. Click on the relevant tab for the task you want to perform and the appropriate fields populate on the page. Retrieve is always the default for tabbed pages.

Figure 2-5 Tabbed Pages



Timestamp	System CPU UtilPct Average	System CPU UtilPct Peak	System Disk UtilPct Average	System Disk UtilPct Peak	System RAM UtilPct Average
10/22/2009 19:45	6.764068	44	0.520000	1	7.939407
10/22/2009 20:00	7.143644	25	0.520000	1	8.523822

Figure 2-6 Tabbed Pages



Reports

Reports provide a formatted display of information. Reports are generated from data tables by clicking **Report**. Reports can be viewed directly on the user interface, or they can be printed. Reports can also be saved to a text file.

Figure 2-7 Report Output

```
================================================================================

User Account Usage Report

================================================================================

Report Generated: Fri Jun 19 19:30:55 2009 UTC
From: Unknown Network OAM&P on host teks5001701
Report Version: 1.0
User: guiadmin

--------------------------------------------------------------------------------

Username          Date of Last Login    Days Since Last Login   Account Status
----------------  --------------------  ----------------------  ---------------
guiadmin          2009-06-19 19:00:17   0                       enabled

--------------------------------------------------------------------------------

End of User Account Usage Report

================================================================================
```

Customizing the Splash Page Welcome Message

When you first log into the user interface, the splash page displays. Located in the center of the main work area is a customizable welcome message. Use this procedure to create a message suitable for your needs.

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Locate **Welcome Message** in the **Variable** column.
3. Enter the desired welcome message text in the **Value** column.
4. Click **OK** to save the change or **Cancel** to undo the change and return the field to the previously saved value.

   A status message displays at the top of the page to inform you if the operation was successful.

The next time you log into the user interface, the new welcome message text displays.

Column Headers (Sorting)

You can sort a table by a column by clicking the column header. However, sorting is not necessarily available on every column. Sorting does not affect filtering.

When you click the header of a column in a table that can be sorted, an indicator displays in the column header showing the direction of the sort. See Figure 2-8. Clicking the column header again reverses the direction of the sort.

Figure 2-8 Sorting a Table by Column Header

Page Controls

User interface pages contain controls, such as buttons and links, that perform specified functions. The functions are described by the text of the links and buttons.

Note: Disabled buttons are grayed out. Buttons that are irrelevant to the selection or current system state, or which represent unauthorized actions as defined in Group Administration, are disabled. For example, **Delete** is disabled for users without Global Data Delete permission. Buttons are also disabled if, for example, multiple servers are selected for an action that can only be performed on a single server at a time.

Table 2-4 contains examples of Action buttons.

Table 2-4 Example Action Buttons

Action Button	Function
Insert	Inserts data into a table.
Edit	Edits data within a table.
Delete	Deletes data from table.
Change	Changes the status of a managed object.

Some Action buttons take you to another page.

Submit buttons, described in Table 2-5, are used to submit information to the server. The buttons are located in the page area and accompanied by a table in which you can enter information. The Submit buttons, except for **Cancel**, are disabled until you enter some data or select a value for all mandatory fields.

Table 2-5 Submit Buttons

Submit Button	Function
OK	Submits the information to the server, and if successful, returns to the View page for that table.
Apply	Submits the information to the server, and if successful, remains on the current page so that you can enter additional data.
Cancel	Returns to the View page for the table without submitting any information to the server.

Clear Field Control

The clear field control allows you to clear the value from a list. The clear field control is available only on some lists.

Click the **X** next to a list to clear the field.

Figure 2-9 Clear Field Control X

Optional Layout Element Toolbar

The optional layout element toolbar displays in the Page Control Area of the GUI.

Figure 2-10 Optional Layout Element Toolbar

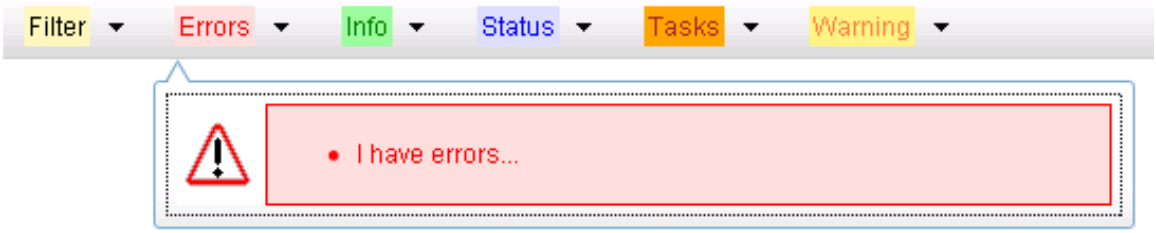
The toolbar displays different elements depending on which GUI page is selected. The elements of the toolbar that can display include:

- Filter – Allows you to filter data in a table.
- Errors – Displays errors associated with the work area.
- Info – Displays information messages associated with the work area.
- Status – Displays short status updates associated with the main work area.
- Warning – Displays warnings associated with the work area.

Notifications

Some messages require immediate attention, such as errors and status items. When new errors occur, the Errors element opens automatically with information about the error. Similarly, when new status items are added, the Status element opens. If you close an automatically opened element, the element stays closed until a new, unacknowledged item is added.

Figure 2-11 Automatic Error Notification



Note: Viewing and closing an error does not clear the Errors element. If you reopen the Errors element, previously viewed errors are still in the list.

When new messages are added to Warning or Info, the styling of the element changes to indicate new messages are available. The styling of the Task element changes when a task changes state (such as, a task begins or ends).

Opening an Element in the Toolbar

Use this procedure to open an element in the optional layout element toolbar.

1. Click the text of the element or the triangle icon to open an element.

   The selected element opens and overlays the work area.

2. Click **X** to close the element display.

Filters

Filters are part of the optional layout element toolbar and appear throughout the GUI in the Page Control Area. For more information about optional layout element toolbar functionality, see Optional Layout Element Toolbar.

Filters allow you to limit the data presented in a table and can specify multiple filter criteria. By default, table rows appear unfiltered. Three types of filters are supported, however, not all filtering options are available on every page. The types of filters supported include:

- Network Element – When enabled, the Network Element filter limits the data viewed to a single Network Element.

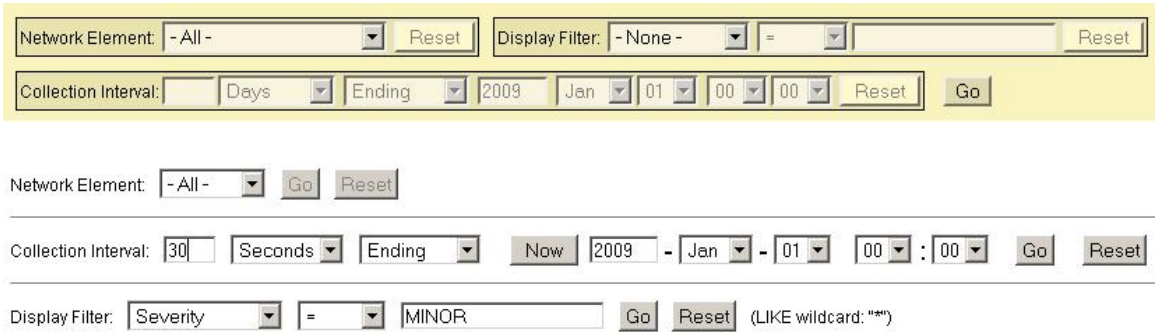
  Note: Once enabled, the Network Element filter affect all pages that list or display data relating to the Network Element.

- Collection Interval – When enabled, the collection interval filter limits the data to entries collected in a specified time range.
- Display Filter – The display filter limits the data viewed to data matching the specified criteria.

Once a field is selected, it cannot be selected again. All specified criteria must be met in order for a row to be displayed.

The style or format of filters may vary depending on which GUI pages the filters are displayed. Regardless of appearance, filters of the same type function the same.

Figure 2-12 Examples of Filter Styles



Filter Control Elements

This table describes filter control elements of the user interface.

Table 2-6 Filter Control Elements

Operator	Description
=	Displays an exact match.
!=	Displays all records that do not match the specified filter parameter value.
>	Displays all records with a parameter value that is greater than the specified value.

Table 2-6 (Cont.) Filter Control Elements

Operator	Description
>=	Displays all records with a parameter value that is greater than or equal to the specified value.
<	Displays all records with a parameter value that is less than the specified value.
<=	Displays all records with a parameter value that is less than or equal to the specified value.
Like	Enables you to use an asterisk (*) as a wildcard as part of the filter parameter value.
Is Null	Displays all records that have a value of **Is Null** in the specified field.

Note: Not all filterable fields support all operators. Only the supported operators are available for you to select.

Filtering on the Network Element

The global Network Element filter is a special filter that is enabled on a per-user basis. The global Network Element filter allows a user to limit the data viewed to a single Network Element. Once enabled, the global Network Element filter affects all sub-screens that display data related to Network Elements. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
2. Select a Network Element from the **Network Element** list.
3. Click **Go** to filter on the selection or click **Reset** to clear the selection.
4. For data tables that support compound filtering, click **Add** to add another filter condition and repeat steps 2 through 4.

   Multiple filter conditions are joined by an AND operator.

Records are displayed according to the specified criteria.

Filtering on Collection Interval

The Collection Interval filter allows a user to limit the data viewed to a specified time interval. This filtering option may not be available on all pages.

1. Click **Filter** in the optional layout element toolbar.
2. Enter a duration for the **Collection Interval** filter.

   The duration must be a numeric value.

3. Select a unit of time from the list.

   The unit of time can be seconds, minutes, hours, or days.

4. Select **Beginning** or **Ending** from the list.

5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Filtering Using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes you have a data table displayed on your screen with the Display Filter field. This process is the same for all data tables. However, all filtering operations are not available for all tables.

> **Note:** Display Filter does not support compound filtering. For example, you cannot filter on both severity and a server name. Try to filter on a single filter criteria, such as the server hostname for server-scoped metric cells; or the application name for St- and NE-scoped metric cells. You can also sort by congestion level (descending) to help improve your filter.

1. Click **Filter** in the optional layout element toolbar.

2. Select a field name from the **Display Filter** list.

   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

3. Select an operator from the operation selector list.

4. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify Filter=Severity with the equals (=) operator and a value of MINOR, the table would show only records where Severity=MINOR.

5. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

> **Note:** PCA was known as PDRA and may still be seen in some filtering.

Pause Updates

Some pages refresh automatically. Updates to these pages can be paused by selecting the **Pause updates** checkbox. Uncheck the **Pause updates** checkbox to resume automatic updates. The **Pause updates** checkbox is available only on some pages.

Max Records Per Page Controls

Max Records Per Page is used to control the maximum number of records displayed in the page area. If a page uses pagination, the value of Max Records Per Page is used. Use this procedure to change the Max Records Per Page.

1. From the **Main Menu**, click **Administration** > **General Options**.
2. Change the value of the **MaxRecordsPerPage** variable.

   Note: **Maximum Records Per Page** has a range of values from 10 to 100 records. The default value is 20.

3. Click **OK** or **Apply**.

   OK saves the change and returns to the previous page.

   Apply saves the change and remains on the same page.

The maximum number of records displayed is changed.

3

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: Some of the alarms in the Operations, Administration, and Maintenance (OAM) and Platform Alarms sections are shared with other applications and may not appear in UDR.

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

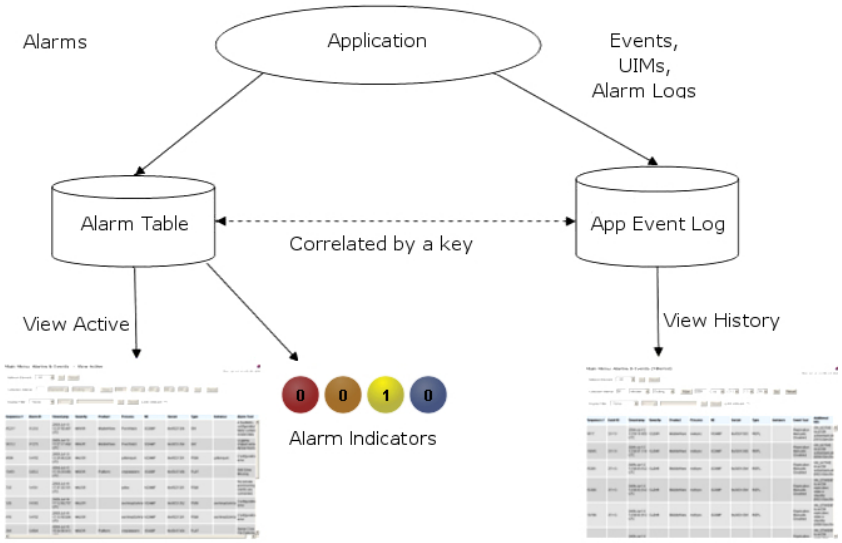
An alarm is considered inactive once it has been cleared and cleared alarms are logged on the Alarms & Events > View History page of the GUI.

Events note the occurrence of a transient condition. 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 (e.g., generating an event for every ingress message failure). By specifying a throttle interval (in seconds), the events will appear no more frequently than once during the interval duration period (e.g., if the throttle interval is 5-seconds, the event will be logged no frequently than once every 5-seconds).

Figure 3-1 shows how Alarms and Events are organized in the application.

Figure 3-1 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 that represent 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, that means there are six major active alarms.

Figure 3-2 Alarm Indicators Legend

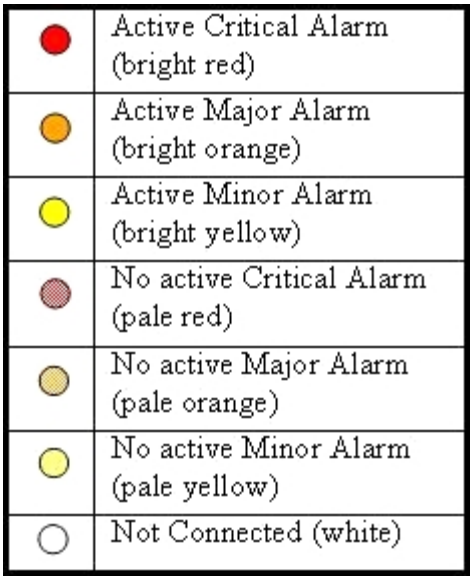
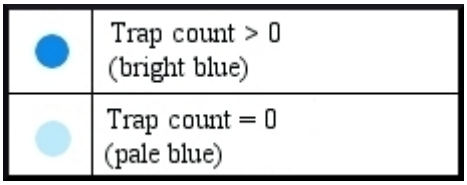


Figure 3-3 Trap Count Indicator Legend



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 that 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 3-1.

Table 3-1 Alarm/Event ID Ranges

Application/Process Name	Alarm ID Range
IPFE	5000-5099
OAM	10000-10999
IDIH	11500-11549
ComAgent	19800-19909
DSR Diagnostics	19910-19999
Diameter	8000-8299, 22000-22350, 22900-2999, 25500-25899
RBAR	22400-22424
Generic Application	22500-22599
FABR	22600-22640
PDRA	22700-22799
TVOE	24400-24499
CAPM	25000-25499
OAM Alarm Management	25500-25899
Platform	31000-32700
DM-IWF	33000-33024
Load Generator	33025-33049
MD-IWF	33050-33099
GLA	33100-3149
DCA	33300-33630
I-SBR	33730-33830

Alarm and event types

Table 3-2 describes the possible alarm/event types that can be displayed.

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

Table 3-2 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

Table 3-2 (Cont.) Alarm and Event Types

Type Name	Type
PROC	Process
PROV	Provisioning
pSBR	Policy SBR
QP	QBus
RBAR	Range-Based Address Resolution
REPL	Replication
SCTP	Stream Control Transmission Protocol
SDS	Subscriber Database Server
SIGC	Signaling Compression
SIP	Session Initiation Protocol Interface
SL	Selective Logging
SS7	Signaling System 7
SSR	SIP Signaling Router
STK	EXG Stack
SW	Software (generic event type)
TCP	Transmission Control Protocol

Viewing 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 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** > **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

This table describes the elements on the **View Active** > **Export** alarms page.

Table 3-3 Schedule Active Alarm 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.
Export Frequency	Frequency at which the export occurs	Format: Option Range: Once, Fifteen Minutes, Hourly, Daily, or Weekly 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: Option Range: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday Default: Sunday

Exporting active alarms

You can schedule periodic exports of alarm data from the Alarms and Events 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.

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.

Alarm details can be exported to a file by clicking the **Export** button 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.

If filtering has been applied in the View Active page, only filtered, active alarms are exported.

Use this procedure to export active alarms to a file.Use this procedure to schedule a data export task.

1. Select **Alarms & Events** > **View Active**.

   The View Active page appears.

2. If necessary, specify filter criteria and click **Go**.

   The active alarms are displayed according to the specified criteria.

3. Click **Export**.

   The Schedule Active Alarm Data Export page appears.

4. Enter the **Task Name**.

   For more information about **Task Name**, or any field on this page, see Active alarms data export elements.

5. Select the **Export Frequency**.

6. Select the **Time of Day**.

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

7. Select the **Day of Week**.

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

8. Click **OK** or **Apply** to initiate the active alarms export task.

   From the **Status & Manage** > **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see Viewing the file list.

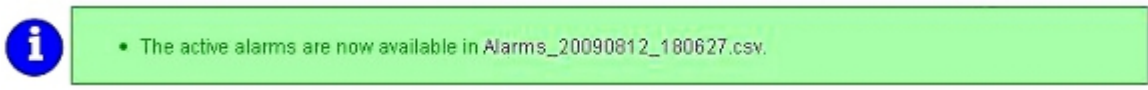
   Scheduled tasks can be viewed, edited, and deleted, and reports of scheduled tasks can be generated from **Status & Manage** > **Tasks**. For more information see:

- Viewing scheduled tasks
- Editing a scheduled task
- Deleting a scheduled task
- Generating a scheduled task report

9. Click **Export**.

   The file is exported.

10. Click the link in the green message box to go directly to the Status & Manage > Files page.



   From the **Status & Manage** > **Files** page, you can view a list of files available for download, including the active alarms file you exported during this procedure.

Generating a report of active alarms

Use this procedure to generate a report.

1. Click **Alarms & Events** > **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.

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** > **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 appears. Click **More** to view a report that displays 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 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.

Historical events data export elements

This table describes the elements on the **View History** > **Export** page.

Table 3-4 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.
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

Table 3-4 (Cont.) Schedule Event Data Export Elements

Element	Description	Data Input Notes
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** > **View History**.

   The View History page appears.

2. If necessary, specify filter criteria and click **Go**.

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

3. Click **Export**.

   The Schedule Event Data Export page appears.

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** > **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 Viewing the file list.

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

   - Viewing scheduled tasks
   - Editing a scheduled task
   - Deleting a scheduled task
   - Generating a scheduled task report

10. Click **Export**.

    The file is exported.

11. Click the link in the green message box to go directly to the **Status & Manage** > **Files** page.

    From the **Status & Manage** > **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** > **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.

Viewing 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** > **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** > **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:

- Exporting 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** > **Remote Servers** > **Data Export** page.

Table 3-5 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)

Table 3-5 (Cont.) Data Export Elements

Element	Description	Data Input Notes
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
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** > **Remote Servers** > **Data Export**.
2. Enter a **Hostname**.

   See Data Export elements for details about the **Hostname** field and other fields that appear 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 that are 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 3-6 describes elements on the Active Tasks page.

Table 3-6 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** > **Tasks** > **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** > **Tasks** > **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** > **Tasks** > **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** > **Tasks** > **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** > **Tasks** > **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 3-7 describes elements on the Active Tasks [Report] page.

Table 3-7 Active Tasks Report Elements

Active Tasks Report Element	Description
Task ID	Task ID
Display Name	Task name

Table 3-7 (Cont.) Active Tasks Report Elements

Active Tasks Report Element	Description
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** > **Tasks** > **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:

- Exporting active alarms

- Exporting alarm and event history
- Exporting KPIs

Viewing scheduled tasks

Use this procedure to view the scheduled tasks.

1. Select **Status & Manage** > **Tasks** > **Scheduled Tasks**.

   The Scheduled Tasks page appears, and all scheduled tasks are displayed.

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 3-8 describes elements on the Scheduled Tasks page.

Table 3-8 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** > **Tasks** > **Scheduled Tasks**.

   All scheduled tasks are displayed on the Scheduled Tasks page.

2. Select a task.
3. Click **Edit**.

   The Data Export page for the selected task appears.

4. Edit the available fields as necessary.

   See Scheduled Tasks elements for details about the fields that appear 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** > **Tasks** > **Scheduled Tasks**.

   All scheduled tasks are displayed on the Scheduled Tasks page.

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** > **Tasks** > **Scheduled Tasks**.

   All scheduled tasks are displayed on the Scheduled Tasks page.

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.

4

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 the Alarms & Events > View Active GUI menu option. The alarms and events log can be viewed from the View History GUI menu 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

Recovery:

1. Check the status of the application servers by navigating to the **Status & Manage** > **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 for assistance.

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

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** > **Configuration** > **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 the **Configuration** > **Network** > **Devices** All IPFE Server tab and **IPFE** > **Configuration** > **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** > **Configuration** > **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

Recovery:

1. Check IPFE server configurations by navigating to **IPFE** > **Configuration** > **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** > **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 for the **Configuration** > **Network** > **Devices** All IPFE Server tab and **IPFE** > **Configuration** > **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

Recovery:

1. Navigate to **IPFE** > **Configuration** > **Options**.

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

2. From the Configuration Options screen, navigate to **IPFE** > **Configuration** > **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

Recovery:

1. When the IPFE receives heartbeats from the application server indicating that 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

Recovery

1. Navigate to **Status & Manage** > **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

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 more 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

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** > **Server** page.
3. Consult the application server's documentation for recovery steps.
4. It is recommended to contact My Oracle Support.

5009 - No available servers in target set

Alarm Group:
IPFE

Description:
Through monitoring of the application servers, the IPFE 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

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** > **Configuration** > **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** > **Configuration** > **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

Recovery:

1. 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** > **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** > **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 that 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

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** > **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 for assistance.

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, e.g., bond0.5.

HA Score:
Degraded

Auto Clear Seconds:
N/A

OID:
ipfeIpfeSignalingInterfaceNotify

Recovery:

1. Check if any manual configuration changes have been executed that remove 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. If the problem persists, it is recommended to contact My Oracle Support.

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

Recovery:

1. If no packets have been dropped for five seconds, the alarm clears.
2. If the problem persists, it is recommended to contact My Oracle Support.

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

Recovery:

1. The product 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 for assistance.

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

Recovery:

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

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

Recovery:

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

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

Recovery:

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

OAM (10000-10999)

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

10000 - Incompatible database version

Alarm Group:
DB

Description:
The database version is incompatible with the installed software database version.

> **Note:** As of AppWorks 5.0, this alarm is no longer used.

Severity:
Critical

Instance:
N/A

HA Score:
Failed

Auto Clear Seconds:
300

OID:
tekelecIncompatibleDatabaseVersionNotify

Recovery:

1. It is recommended to contact My Oracle Support.

10001 - Database backup started

Event Type:
DB

Description:
The database backup has started.

Severity:
Info

Instance:
GUI

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecBackupStartNotify

Recovery:

1. No action action required.

10002 - Database backup completed

Event Type:
DB

Description:
Backup completed

Severity:
Info

Instance:
GUI

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecBackupCompleteNotify

Recovery:

1. No action required.

10003 - Database backup failed

Event Type:
DB

Description:
The database backup has failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecBackupFailNotify

Recovery:

1. It is recommended to contact My Oracle Support.

10004 - Database restoration started

Event Type:
DB

Description:
The database restoration has started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecRestoreStartNotify

Recovery:

1. No action required.

10005 - Database restoration completed

Event Type:
DB

Description:
The database restoration is completed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecRestoreCompleteNotify

Recovery:

1. No action required.

10006 - Database restoration failed

Event Type:
DB

Description:
The database restoration has failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecRestoreFailNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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

Recovery:

1. No action required.

10009 - Config and Prov db not yet synchronized

Alarm Group:
REPL

Description:
The configuration and the 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 state, can get it from pl command). DB re-initialization fails because the remote server is not in the correct state, for example, it is not in OOS state.

This alarm can also be observed during some DSR patch installation 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 alarm 10009 when applying the patch.

Severity:
Critical

Instance:
N/A

HA Score:
Failed

Auto Clear Seconds:
This alarm does not autoclear.

OID:
oAGTCfgProvDbNoSyncNotify

Recovery:

1. Monitor the replication status by navigating to **Status & Manage** > **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.

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

Recovery:

1. If alarm persists for more than 30 seconds, it is recommended to contact My Oracle Support.

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:
oAGTCantMonitorTableNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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:
oAGTResponderFailedNotify

Recovery:

1. It is recommended to contact My Oracle Support.

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

Recovery:

1. If duration of alarm is greater than two seconds, it is recommended to contact My Oracle Support.

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

Recovery:

1. Alarm will clear if a backup (Automated or Manual) of the same group data is successful. It is recommended to contact My Oracle Support if failures persist.

10050 - Resource Audit Failure

Alarm Group:
AUD

Description:
Database backup failed.

Severity:
Minor

Instance:

HA Score:
Normal

Auto Clear Seconds:
0

OID:
awpss7TekelecResourceAuditFailureNotify

Recovery:

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

10051 - Route Deployment Failed

Alarm Group:
AUD

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

Severity:
Minor

Instance:
Route ID failed to deploy

HA Score:
Normal

Auto Clear Seconds:
0

OID:
awpss7TekelecRouteDeploymentFailedNotify

Recovery:

1. Try restarting the apwSoapServer service on the affected server.
2. If the alarm persists, collect trace list in Diagnostic Information and it is recommended to contact My Oracle Support.

10052 - Route Discovery Failed

Alarm Group:
AUD

Description:
An error occurred in the discovery of network routes.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
awpss7TekelecRouteDiscoveryFailedNotify

Recovery:

1. Try restarting the apwSoapServer service on the affected server.
2. If the problem persists, it is recommended to contact My Oracle Support.

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

OID:
awpss7TekelecNoRouteDeviceNotify

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

OID:
awpss7TekelecDeviceDeploymentFailedNotify

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 more assistance is needed.

10055 - Device discovery failed

Alarm Group:
AUD

Description:
An error occurred in the discovery of network devices.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0

OID:
awpss7TekelecDeviceDiscoveryFailedNotify

Recovery:

1. Correct any directory or file permissions (/etc/sysconfig/network-scripts/*), if required.
2. 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.
3. If the problem persists, it is recommended to contact My Oracle Support.

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

OID:
oAGTSgMaxAllowedHARoleWarnNotify

Recovery:

1. Log into the SO GUI and navigate to the HA page (**Status & Manage** > **HA**).
2. Click the **Edit** button 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** > **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 login to 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

Recovery:

1. No action required; the alarm clears automatically when 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

Recovery:

1. If maintenance actions are complete, restart application processes on the server from the **Status & Manage** > **Servers** page by selecting the Restart Applications action for the server that raised the alarm.

   Once successfully restarted, the alarm will clear.

10078 - Application not restarted on standby server due to disabled failure cleanup mode

Event Type:
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

Throttle Seconds:
1

OID:
failureRecoveryWithoutAppRestartNotify

Recovery:

1. It is recommended to contact My Oracle Support.

10100 - Log export started

Event Type:
LOG

Description:
Log files export operation has started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportStartNotify

Recovery:

1. No action required.

10101 - Log export successful

Event Type:
LOG

Description:
The log files export operation completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportSuccessNotify

Recovery:

1. No action required.

10102 - Log export failed

Event Type:
LOG

Description:
The log files export operation failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportFailedNotify

Recovery:

1. Verify the export request and try the export again.
2. If the problem persists, it is recommended to contact My Oracle Support.

10103 - Log export already in progress

Event Type:
LOG

Description:
Log files export operation not run - export can only run on Active Network OAMP server.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportNotRunNotify

Recovery:

1. Restart export operation after existing export completes.

10104 - Log export file transfer failed

Event Type:
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** > **Tasks** > **Active Tasks**.

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecExportXferFailedNotify

Recovery:

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

10105 - Log export cancelled - user request

Event Type:
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** > **Tasks** > **Active Tasks**.

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportCancelledUserNotify

Recovery:

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

10106 - Log export cancelled - duplicate request

Event Type:
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** > **Tasks** > **Active Tasks**.

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportCancelledDuplicateNotify

Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

10107 - Log export cancelled - queue full

Event Type:
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** > **Tasks** > **Active Tasks**.

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogExportCancelledQueueNotify

Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure the queue does not fill up.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

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** > **Tasks** > **Scheduled Tasks**.

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
tekelecLogExportDupSchedTaskNotify

Recovery:

1. Check the duration and/or frequency of scheduled exports as they are not completing before the next scheduled export is requested.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

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** > **Tasks** > **Active Tasks** or **Status & Manage** > **Tasks** > **Scheduled Tasks**.

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
tekelecLogExportQueueFullNotify

Recovery:

1. Check the amount, duration and/or frequency of scheduled exports to ensure that the queue does not fill up.
2. If the problem persists, it is recommended to contact My Oracle Support for assistance.

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

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 for assistance.

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

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 for assistance.

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

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 for assistance.

10115 - Health Check Started

Event Type:
LOG

Description:
Upgrade health check operation started.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckStart

Recovery:

1. No action required.

10116 - Health Check Successful

Event Type:
LOG

Description:
Upgrade health check operation completed successfully.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckSuccess

Recovery:

1. No action required.

10117 - Health Check Failed

Event Type:
LOG

Description:
Upgrade health check operation failed.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckFailed

Recovery:

1. No action required.

10118 - Health Check Not Run

Event Type:
LOG

Description:
Upgrade health check not run.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogHealthCheckNotRun

Recovery:

1. It is recommended to contact My Oracle Support.

10120 - Server Group Upgrade Started

Event Group:
LOG

Description:
The server group upgrade operation has started.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogSgUpgradeStart

Recovery:

1. No action required.

10121 - Server Group Upgrade Cancelled - Validation Failed

Event Group:
LOG

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

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogSgUpgradeCancelled

Recovery:

1. No action required.

10122 - Server Group Upgrade Successful

Event Group:
LOG

Description:
The server group upgrade operation completed successfully.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogSgUpgradeSuccess

Recovery:

1. No action required.

10123 - Server Group Upgrade Failed

Event Group:
LOG

Description:
The server group upgrade operation failed.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogSgUpgradeFailed

Recovery:

1. 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

Event Group:
LOG

Description:
The user cancelled the server group upgrade operation.

Severity:
Info

Instance:
<ServerGroupName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogSgUpgradeCancelledUser

Recovery:

1. 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:
dbcTekelecLogSgUpgradeFailAlmNotify

Recovery

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

10130 - Server Upgrade Started

Event Group:
LOG

Description:
The server upgrade operation has started.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogServerUpgradeStart

Recovery:

1. No action required.

10131 - Server Upgrade Cancelled

Event Group:
LOG

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

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogServerUpgradeCancelled

Recovery:

1. No action required.

10132 - Server Upgrade Successful

Event Group:
LOG

Description:
The server upgrade operation completed successfully.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogServerUpgradeSuccess

Recovery:

1. No action required.

10133 - Server Upgrade Failed

Event Group:
LOG

Description:
The server upgrade operation failed.

Severity:
Info

Instance:
<HostName>

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogServerUpgradeFailed

Recovery:

1. 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

OID:
tekelecLogServerUpgradeFailAlm

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** > **Software Management** > **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** > **Software Management** > **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 will never upgrade 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** > **Software Management** > **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** > **Software Management** > **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

Event Type:
LOG

Description:
Site upgrade operation started.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeStart

Recovery:

1. No action required.

10141 - Site Upgrade Cancelled

Event Type:
LOG

Description:
Site upgrade cancelled - validation failed.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeCancelled

Recovery:

1. No action required.

10142 - Site Upgrade Successful

Event Type:
LOG

Description:
Site upgrade operation completed successfully.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeSuccess

Recovery:

1. No action required.

10143 - Site Upgrade Failed

Event Type:
LOG

Description:
Site upgrade operation failed.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeFailed

Recovery:

1. 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

Event Type:
LOG

Description:
Site upgrade cancelled by user.

Severity:
Info

Instance:
<SiteName>

HA Score:
Normal

Throttle Seconds:
N/A

OID:
tekelecLogSiteUpgradeCancelledUser

Recovery:

1. 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

Recovery:

1. 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

Event Type:
LOG

Description:
The login operation was successful.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLoginSuccessNotify

Recovery:

1. No action required.

10152 - Login failed

Event Type:
LOG

Description:
The login operation failed

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLoginFailedNotify

Recovery:

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

10153 - Logout successful

Event Type:
LOG

Description:
The logout operation was successful.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecLogoutSuccessNotify

Recovery:

1. 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

Recovery:

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

10155 - SAML Login Successful

Event Group:
LOG

Description:
SAML Login Successful

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecSamlLoginSuccessNotify

Recovery:

1. This is not a failure event. It's an indication that a 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

Event Group:
LOG

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
1

OID:
tekelecSamlLoginFailed

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

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

10300 - SNMP Trapping Not Configured

Alarm Group
DB

Description
SNMP Trapping Not Configured for Site

Severity
Minor

Instance
<Hostname>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
apwSnmpTrappingNotConfiguredForSite

Recovery

1. 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

Recovery:

1. 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

Recovery:

1. No action required

11502 - Troubleshooting Trace Started

Event Group:
IDIH

Description:
A troubleshooting trace instance was started.

Severity:
Info

Instance:
<TraceInstanceId>

HA Score:
Normal

Throttle Seconds:
0

OID:
eagleXgDiameterIDIHTraceStartedNotify

Recovery:

1. No action required.

11503 - Troubleshooting Trace Stopped

Event Group:
IDIH

Description:
A troubleshooting trace instance was stopped.

Severity:
Info

Instance:
<TraceInstanceId>

HA Score:
Normal

Throttle Seconds:
0

OID:
eagleXgDiameterIDIHTraceStoppedNotify

Recovery:

1. 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

Throttle Seconds:
30

OID:
eagleXgDiameterInvalidIDIHTraceAvpNotify

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.

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 will still run at sites that have this entity configured.

Severity:
Info

Instance:
<TraceName>

HA Score:
Normal

Throttle Seconds:
0

OID:
eagleXgDiameterUnableToRunNetworkTraceAtThisSiteNotify

Recovery:

1. No action required; the trace will still run 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

OID
eagleXgDiameterInvalidDihHostNameAlarmNotify

Recovery

1. 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 Type: PROV

Description: Provisioning interface is manually disabled.

Severity: Critical

Instance: N/A

HA Score: Normal

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

OID: sdsProvInterfaceDisabled

Recovery: 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. Alarm clears when one of the ports is changed.

14120 - Connection Established

Event Type
PROV

Description
Provisioning client connection established.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvConnectionEstablished

Recovery

1. No action required for this event.

14121 - Connection Terminated

Event Type
PROV

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

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvConnectionTerminated

Recovery

1. No action required for this event.

14122 - Connection Denied

Event Type
PROV

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

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvConnectionDenied

Recovery

1. No action required for this event.

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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. Correct the problem and try the export again.

14160 - Import Operation Completed

Event Type
PROV

Description
All files were imported successfully.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvImportOperationCompleted

Recovery

1. No action required for this event.

14161 - Export Operation Completed

Event Type
PROV

Description
All scheduled exports completed successfully.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvExportOperationCompleted

Recovery

1. No action required for this event.

14170 - Remote Audit started and in progress

Event Type
PROV

Description
Remote Audit started and is in progress.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvRemoteAuditStartedAndInProgressNotify

Recovery

1. No action required for this event.

14171 - Remote Audit aborted

Event Type
PROV

Description
Remote Audit aborted.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvRemoteAuditAbortedNotify

Recovery

1. No action required for this event.

14172 - Remote Audit failed to complete

Event Type
PROV

Description
Remote Audit failed to complete.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvRemoteAuditFailedToCompleteNotify

Recovery

1. No action required for this event.

14173 - Remote Audit completed

Event Type
PROV

Description
Remote Audit completed successfully.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvRemoteAuditCompletedNotify

Recovery

1. No action required for this event.

14174 - NPA Split pending request deleted

Event Type
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

Throttle Seconds
N/A

OID
sdsProvNpaSplitPendingRequestDeleted

Recovery

1. No action required for this event.

14175 - NPA Split activation failed

Event Type
PROV

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

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvNpaSplitActivationFailed

Recovery

1. Contact the My Oracle Support.

14176 - NPA Split started and is active

Event Type
PROV

Description
NPA Split started and is active.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvNpaSplitActivated

Recovery

1. No action required for this event.

14177 - NPA Split completion failed

Event Type
PROV

Description
NPA Split completion failed. See trace log for details.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvNpaSplitCompletionFailed

Recovery

1. Contact the My Oracle Support.

14178 - NPA Split completed

Event Type
PROV

Description
NPA Split completed.

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
N/A

OID
sdsProvNpaSplitCompleted

Recovery

1. No action required for this event.

14179 - MSISDN deleted from Blacklist

Event Type
PROV

Description
Previously Blacklisted MSISDN is now a Routing Entity

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
0

OID
sdsProvMsisdnDeletedFromBlacklist

Recovery

1. No action necessary.

14180 - IMSI deleted from Blacklist

Event Type
PROV

Description
Previously Blacklisted IMSI is now a Routing Entity

Severity
Info

Instance
N/A

HA Score
Normal

Throttle Seconds
0

OID
sdsProvImsiDeletedFromBlacklist

Recovery

1. 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

OID
sdsProvRelayNotConnectedNotify

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

OID
sdsProvRelayTimeLagNotify

Recovery

1. Contact the My Oracle Support.

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

Recovery

1. 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

Recovery

1.

- 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

Recovery

1. Contact the My Oracle Support.

SS7/Sigtran Alarms (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 RSP status is unavailable.

Severity:
Critical

Instance:
RSP Name

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlRspUnavailableNotify

Recovery:

1. RSP/Destination status can be monitored from the SOAM GUI by navigating to **SS7/Sigtran** > **Maintenance** > **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** > **Maintenance** > **Link Sets** to check the status of linkset links to the adjacent server.
3. Navigate to **Transport Manager** > **Maintenance** > **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.

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

Recovery:

1. Route status can be monitored from **SS7/Sigtran** > **Maintenance** > **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 that 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.

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

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** > **Maintenance** > **Linksets**.
3. Verify that 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 that the adjacent server is not under maintenance.
6. If the problem persists, it is recommended to contact My Oracle Support.

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

Recovery:

1. The MP server will attempt to automatically recover all links not manually disabled.
2. Link status can be monitored from **SS7/Sigtran** > **Maintenance** > **Links**.
3. Verify that 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 that the adjacent server is not under maintenance.
6. If the problem persists, it is recommended to contact My Oracle Support.

19204 - Preferred route unavailable

Alarm Group:
SS7

Description:
M3RL 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:
RSP Name

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlPreferredRouteUnavailableNotify

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** > **Maintenance** > **Remote Signaling Points**.
3. Verify that 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 that the adjacent server is not under maintenance.
6. If the problem persists, it is recommended to contact My Oracle Support.

19205 - TFP received

Event Type:
SS7

Description:
The **TFP** message was received by **M3RL** layer; an adjacent point code has reported that it has no longer has any available routes to the **RSP**/Destination.

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7M3rlTfpReceivedNotify

Recovery:

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

19206 - TFA received

Event Type:
SS7

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7M3rlTfaReceivedNotify

Recovery:

1. Monitor the RSP/Destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.

19207 - TFR received

Event Type:
SS7

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7M3rlTfrReceivedNotify

Recovery:

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

19208 - TFC received

Event Type:
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

HA Score:
Normal

Throttle Seconds:
30

Instance:
N/A

OID:
awpss7M3rlTfcReceivedNotify

Recovery:

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

19209 - M3RL routing error

Event Type:
SS7

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
10

OID:
awpss7M3rlRoutingFailureNotify

Recovery:

1. Each MP's assigned point code can be monitored from **SS7/Sigtran** > **Configuration** > **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 that 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 that a route exists for the DPC, and use the RSP status screen to verify that 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 for assistance.

19210 - M3RL routing error - invalid NI

Event Type:
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 that the CDPA is encoded as per international specifications:
  - A "0" in Bit 8 indicates that the address is international and that both the address indicator and the address are coded according to international specifications.
  - A "1" in Bit 8 indicates that the address is national and that 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

Throttle Seconds:
10

OID:
awpss7M3rlRoutingFailureInvalidNiNotify

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** > **Configuration** > **Remote Signaling Points**.
2. If the problem persists, it is recommended to contact My Oracle Support.

19211 - M3RL routing error - invalid SI

Event Type:
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

Throttle Seconds:
10

OID:
awpss7M3rlRoutingFailureInvalidSiNotify

Recovery:

1. If the SI received is not a **0** (SNM) or **3** (SCCP), verify that 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.

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

Recovery:

1. On the active SO, navigate to **SS7/Sigtran** > **Maintenance** > **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** > **Maintenance** > **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** > **View Active** and **Alarms & Events** > **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.

19226 - Timedout waiting for ASP-UP-ACK

Event Type:
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

Throttle Seconds:
10

OID:
awpss7TimedOutWaitingForAspUpAckNotify

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.

19227 - Received unsolicited ASP-DOWN-ACK

Event Type:
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 that 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

Throttle Seconds:
30

OID:
awpss7ReceivedUnsolicitedAspDownAckNotify

Recovery:

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

19229 - Timed out waiting for ASP-ACTIVE-ACK

Event Type:
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

Throttle Seconds:
10

OID:
awpss7TimedOutWaitingForAspActiveAckNotify

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.

19230 - Received unsolicited ASP-INACTIVE-ACK

Event Type:
SS7

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

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7ReceivedUnsolicitedAspInactiveAckNotify

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.

19231 - Received invalid M3UA message

Event Type:
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

Throttle Seconds:
10

OID:
awpss7ReceivedInvalidM3uaMessageNotify

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.

19233 - Failed to send non-DATA message

Event Type:
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

Throttle Seconds:
10

OID:
awpss7FailedToSendNonDataMessageNotify

Recovery:

1. Select **Alarms & Events** > **View History** and check the event history logs for additional SS7 events or alarms from this MP server.
2. Verify that 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.

19234 - Local link maintenance state change

Event Type:
SS7

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

Severity:
Info

Instance:
<LinkName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awpss7LocalLinkMaintenanceStateChangeNotify

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.

19235 - Received M3UA error

Event Type:
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

Throttle Seconds:
10

OID:
awpss7ReceivedM3uaErrorNotify

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 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 (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 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 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.

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

Recovery:

1. You can monitor destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points** and RMU/subsystem status from **SS7/Sigtran** > **Maintenance** > **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 that IP network connectivity exists between the MP server and the adjacent servers.
3. Select **Alarms & Events** > **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 that 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.

19241 - SCCP malformed or unsupported message

Event Type:
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

Throttle Seconds:
30

OID:
awpss7SccpMsgTypeUnrecognizedNotify

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.

19242 - SCCP Hop counter violation

Event Type:
SS7

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

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7SccpHopCounterViolationNotify

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.

19243 - SCCP routing failure

Event Type:
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

Throttle Seconds:
30

OID:
awpss7SccpRoutingFailureNotify

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.

19244 - SCCP routing failure network status

Event Type:
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

Throttle Seconds:
30

OID:
awpss7SccpRoutingFailureNetworkStatusNotify

Recovery:

1. Monitor status on the GUI Main Menu as follows:
   - Destination status from **SS7/Sigtran** > **Maintenance** > **Remote Signaling Points**.
   - RMU/subsystem status from **SS7/Sigtran** > **Configuration** > **Remote MTP3 Users**.
   - Local subsystem status from **SS7/Sigtran** > **Maintenance** > **Local SCCP Users**.
2. Verify that 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 that the adjacent server is not under maintenance.
5. If the problem persists, it is recommended to contact My Oracle Support.

19245 - SCCP GTT failure

Event Type:
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

Throttle Seconds:
10

OID:
awpss7SccpGttFailureNotify

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.

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

Recovery:

1. To clear the alarm:
   a. On the SOAM GUI, select **SS7/Sigtran** > **Configuration** > **Local SCCP Users**.
   b. 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.
   c. Click **Enable** to put the appropriate local SSN in the enabled state.

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

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

19248 - SCCP Segmentation Failure

Event Type:
SS7

Description:
SCCP Segmentation Procedure Failure

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7SccpSegmentationFailureNotify

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 for assistance.

19249 - SCCP Reassembly Failure

Event Type:
SS7

Description:
SCCP Reassembly Procedure Failure

Severity:
Info

Instance:
N/A

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7SccpReassemblyFailureNotify

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 for assistance.

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** > **View Active.**

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7Ss7ProcessCpuUtilizationNotify

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** > **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** > **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** > **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** > **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support.

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** > **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7IngressMsgRateNotify

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** > **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** > **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** > **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.

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** > **View Active**.

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

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7PduBufferPoolUtilNotify

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** > **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** > **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** > **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** > **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support.

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** > **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7SccpStackEventQueueUtilNotify

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** > **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** > **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** > **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** > **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support.

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** > **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlStackEventQueueUtilNotify

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** > **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** > **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** > **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** > **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support.

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** > **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3rlNetMgmtEventQueueUtilNotify

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** > **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** > **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** > **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** > **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support.

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** > **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7M3uaStackEventQueueUtilNotify

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** > **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** > **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** > **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** > **View Active**.
5. If the problem persists, it is recommended to contact My Oracle Support.

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** > **View Active**.

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
This alarm does not autoclear.

OID:
awpss7SctpAggregateAssocWriteQueueUtilNotify

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** > **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** > **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** > **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** > **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.

19259 - Operation discarded due to local resource limitation

Event Type:
SS7

Description:
Operation discarded due to local resource limitation.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapOpDiscardedLocalResLimitNotify

Recovery:

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

19260 - Transaction could not be delivered to remote TCAP peer due to conditions in the network

Event Type:
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

Throttle Seconds:
30

OID:
awpss7TcapTransNotDeliveredToPeerNotify

Recovery:

1. This event indicates that 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 that 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 for assistance if needed.

19262 - Operation discarded due to malformed component received from remote TCAP peer

Event Type:
SS7

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

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapMalformedComponentFromRemoteNotify

Recovery:

1. This event indicates that 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 for assistance if needed.

19263 - Transaction discarded due to malformed dialogue message received from local TC User

Event Type:
SS7

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

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapMalformedDialogueFromLocalNotify

Recovery:

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

19264 - Transaction discarded due to malformed dialogue message from remote TCAP peer

Event Type:
SS7

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

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapMalformedDialogueFromRemoteNotify

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 for assistance if needed.

19265 - Unexpected event received from local TC User

Event Type:
SS7

Description:
Unexpected event received from local TC User.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapUnexpectedMsgFromLocalNotify

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 for assistance if needed.

19266 - Unexpected event received from remote TCAP peer

Event Type:
SS7

Description:
Unexpected event received from remote TCAP peer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapUnexpectedMsgFromRemoteNotify

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
   - 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 for assistance if needed.

19267 - Dialogue removed by dialogue cleanup timer

Event Type:
SS7

Description:
Dialogue removed by dialogue cleanup timer.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapDialogueRemovedTimerExpiryNotify

Recovery:

1. This event indicates that 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 prior to this event indicating that a message could not be routed. If SCCP failed to route the message, verify that 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 for assistance if needed.

19268 - Operation removed by invocation timer expiry

Event Type:
SS7

Description:
Operation removed by invocation timer expiry.

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapOperationRemovedTimerExpiryNotify

Recovery:

1. This event indicates that 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 prior to this event indicating that a message could not be routed. If SCCP failed to route the message, verify that 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 that the component was created, but never sent.
6. It is recommended to contact My Oracle Support for assistance if needed.

19269 - Dialogue aborted by remote TCAP peer

Event Type:
SS7

Description:
Dialogue aborted by remote TCAP peer

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapDialogueAbortByRemoteNotify

Recovery:

1. This event indicates that 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 for assistance if needed.

19270 - Received unsupported TCAP message

Event Type:
SS7

Description:
Received unsupported TCAP message

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapUnsupportedTCAPMsgRcvdNotify

Recovery:

1. This event indicates that 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 for assistance if needed.

19271 - Operation rejected by remote TCAP peer

Event Type:
SS7

Description:
Operation rejected by remote TCAP peer

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapReturnRejectByRemoteNotify

Recovery:

1. This event indicates that 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 for assistance if 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 clear automatically)

OID:
awpss7TcapActiveDialogueUtilNotify

Recovery:

1. The percent utilization of the MP's dialogue table is approaching maximum capacity. This alarm indicates that 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 for assistance if 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 clear automatically)

OID:
awpss7TcapActiveOperationUtilNotify

Recovery:

1. The percent utilization of the MP's component table is approaching maximum capacity. This alarm indicates that 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 for assistance if 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 clear automatically)

OID:
awpss7TcapStackEventQueueUtilNotify

Recovery:

1. The percent utilization of the MP's TCAP Stack Event Queue is approaching its maximum capacity. This alarm indicates that 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 for assistance if needed.

19275 - Return error from remote TCAP peer

Event Type:
SS7

Description:
Return error from remote TCAP peer

Severity:
Info

Instance:
Application name

HA Score:
Normal

Throttle Seconds:
30

OID:
awpss7TcapReturnErrorFromRemoteNotify

Recovery:

1. This event indicates that 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 for assistance if 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 clear automatically)

OID:
awpss7SccpEgressMsgRateNotify

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 for assistance if needed.

19281 - TCAP Routing Failure

Event Type:
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

Throttle Seconds:
10

OID:
awpss7TcapRoutingFailureNotify

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 for assistance if needed.

Transport Manager Alarms and Events (19400-19419)

This section provides information and recovery procedures for Transport Manager alarms and events, ranging from 19400-19499.

19400 - Transport Down

Alarm Group:
TMF

Description:
Transport Down

Severity:
Major

Instance:
<TransportName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
awptransmgrTransportDownNotify

Recovery:

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

   Additional Information for the alarm can be found in **Alarms & Events** > **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** > **Maintenance** > **'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 that the association's local IP address and port number are configured on the IP Signaling Gateway (Some Signaling Gateways will only accept

connections from IP addresses and ports that they are configured to accept from).

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

2. If the alarm persists, it is recommended to contact My Oracle Support.

19401 - Failed to configure Transport

Event Type:
TMF

Description:
Failed to configure Transport

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awptransmgrFailedToConfigureTransportNotify

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 for assistance.

19402 - Failed to connect Transport

Event Type:
TMF

Description:
Failed to connect Transport

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
60

OID:
awptransmgrFailedToConnectTransportNotify

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 that the transport's local IP address and port number are configured on the Adjacent Node (Some Nodes will only accept connections from IP addresses and ports they are configured to accept connections from).
   - Verify that the transport's remote IP address and port correctly identify an SCTP listening port on the adjacent node.
   - Verify that IP network connectivity exists between the MP and the adjacent node.
   - Verify that 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** > **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.

19403 - Received malformed SCTP message (invalid length)

Alarm Group:
TMF

Description:
Received malformed SCTP message (invalid length).

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awptransmgrReceivedMalformedTransSctpMessageNotify

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.

19404 - Far-end closed the Transport

Event Type:
TMF

Description:
Far-end closed the Transport

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
10

OID:
awptransmgrFarEndClosedTheTransportNotify

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.

19405 - Transport closed due to lack of response

Event Type:
TMF

Description:
Transport closed due to lack of response

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
10

OID:
awptransmgrTransportClosedDueToLackOfResponseNotify

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 that IP network connectivity still exists between the MP server and the adjacent server.
   - Verify that 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 fuctioning correctly.
   - Check the event history logs at **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
   - Verify that the adjacent server on the Signaling Gateway is not under maintenance.

2. If the alarm persists, it is recommended to contact My Oracle Support.

19406 - Local Transport maintenance state change

Event Type:
TMF

Description:
Local Transport maintenance state change

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awptransmgrLocalTransportMaintenanceStateChangeNotify

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 **Main Menu** > **Transport Manager** > **Maintenance** > **Transport**.

2. If the alarm persists, it is recommended to contact My Oracle Support.

19407 - Failed to send Transport DATA Message

Event Type:
TMF

Description:
Failed to send Transport DATA Message

Severity:
Info

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

HA Score:
Normal

Throttle Seconds:
10

OID:
awptransmgrFailedToSendTransDataMessageNotify

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 **Main Menu** > **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
   - Verify that 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.

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

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 form **Main Menu** > **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 form **Main Menu** > **Status & Manage** > **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 **Main Menu** > **Status & Manage** > **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.

19409 - Message Rejected by ACL Filtering

Event Type:
TMF

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

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
10

OID:
awptransmgrMessageRejectedByAclFilteringNotify

Recovery:

1. Verify that 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.

19410 - Adjacent Node IP Address state change

Event Type:
TMF

Description:
State change of an IP Address of a multihomed Adjacent Node in SCTP Transport

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awptransmgrAdjIpAddrStateChangeNotify

Recovery:

1. Verify that 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.

19411 - SCTP Transport closed due to failure of multihoming validation

Event Type:
TMF

Description:
SCTP Transport closed due to failure of multihoming validation.

Severity:
Info

Instance:
<TransportName>, <TransportId>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awptransmgrSctpTransportRefusedNotify

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.

19412 - SCTP Transport configuration mismatched for Adjacent Node IP

Event Type:
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

Throttle Seconds:
0 (zero)

OID:
awptransmgrSctpTransportCfgMismatchNotify

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.

19413 - SCTP Transport closed due to unsupported peer address event recieved

Alarm Group:
TMF

Description:
SCTP Transport closed due to unsupported add/delete peer IP Address event recieved in Peer Address Notification.

Severity:
Info

Instance:
<TransportName>

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
awptransmgrTransportClosedDueToUnsupportedEventNotify

Recovery:

1. Disable SCTP Dynamic Address Reconfiguration at the Adjacent Node.
2. If the alarm persists, it is recommended to contact My Oracle Support.

Communication Agent, ComAgent (19420-19909)

This section provides information and recovery procedures for **Communication Agent** (**ComAgent**) alarms and events, ranging from 19800 - 19909, 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 > View Active GUI menu option. The alarms and events log can be viewed from the Alarms & Events > View History page.

19420 - BDFQFull

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

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

19421 - BDFThrotl

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

Recovery:

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

19422 - BDFInvalidPkt

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

Recovery:

1. If more messages of the same type occur, then check the site(s) and network for other possible corruption or overloaded conditions. 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

Recovery:

1. Navigate to **Main Menu** > **Alarms & Events** > **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 **Main Menu** > **Alarms & Events** > **View History** for additional **Communication Agent** events or alarms from this **MP** server.

3. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **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

Recovery:

1. Use **Main Menu** > **Alarms & Events** > **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 **Main Menu** > **Alarms & Events** > **View History** for additional **Communication Agent** events or alarms from this **MP** server.

3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **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 **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screen and click the 'Enable' action button 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

Recovery:

1. Use **Main Menu** > **Alarms & Events** > **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 **Main Menu** > **Alarms & Events** > **View History** for additional **Communication Agent** events or alarms from this **MP** server.

3. Use **Main Menu** > **Communication Agent** > **Maintenance** > **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 **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** screen and click the 'Enable' action button 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

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 event queue. It is recommended to contact My Oracle Support for assistance.

2. Navigate to **Status & Manage** > **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

Recovery:

1. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **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 **Main Menu** > **Alarms & Events** > **View History** for additional **Communication Agent** events or alarms from this **MP** server.
3. Check **Main Menu** > **Communication Agent** > **Maintenance** > **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

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 **Main Menu** > **Alarms & Events** > **View History** for additional **Communication Agent** events or alarms from this **MP** server.
3. Find additional information for the alarm in **Main Menu** > **Alarms & Events** > **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 **Main Menu** > **Alarms & Events** > **View History** for additional Communication Agent events or alarms from this MP server.
5. Check **Main Menu** > **Communication Agent** > **Maintenance** > **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

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** > **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

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** > **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

Recovery:

1. Use **Main Menu** > **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** > **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

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** > **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

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** > **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

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** > **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

Recovery:

1. Use **Main Menu** > **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

Recovery:

1. Use **Main Menu** > **Alarms & Events** and examine the alarm log.
2. Use **Main Menu** > **Security Log** and examine the alarm log.
3. If the event shows up in **Main Menu** > **Alarms & Events**, without the corresponding GUI security-log in **Main Menu** > **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

Recovery:

1. 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

Recovery:

1. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the reasons why connections are unavailable.
3. Navigate to **Main Menu** > **Status & Manage** > **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

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the reasons why connections are unavailable.
3. Use **Main Menu** > **Status & Manage** > **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

Recovery:

1. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Navigate to **Main Menu** > **Communication Agent** > **Maintenance** > **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

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Routed Service Status** to view the connection groups and connections associated with the Routed Service.
2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to view the reasons why connections are unavailable.
3. Use **Main Menu** > **Status & Manage** > **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

Recovery:

1. Navigate to **Status & Manage** > **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

Recovery:

1. Navigate to **Status & Manage** > **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

Recovery:

1. Navigate to **Alarms & Events** > **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** > **View History** to check the event history logs for additional Communication Agent events or alarms from this MP server.
3. Navigate to **Communication Agent** > **Maintenance** > **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

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

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.

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

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

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **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 **Main Menu** > **Communication Agent** > **Maintenance** > **Connection Status** to trouble-shoot the cause of server overload.
3. Check the **Main Menu** > **Communication Agent** > **Maintenance** > **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

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** > **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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **HA Services Status** to determine which sub-resources are unavailable or degraded for the server that asserted the alarm.

2. Use **Main Menu** > **Communication Agent** > **Maintenance** > **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

Recovery:

1. Navigate to **Communication Agent** > **Maintenance** > **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** > **Maintenance** > **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

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

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** > **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

Recovery:

1. 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

Recovery:

1. Use **Main Menu** > **Communication Agent** > **Maintenance** > **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

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

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

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

Recovery:

1. Use **Alarms & Events** > **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** > **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:
CAFDaemonScriptFailureNotify

Recovery:

1. Use **Alarms & Events** > **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 **Main Menu** > **Alarms & Events** > **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

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

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

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

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

Recovery:

1. 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

Recovery:

1. 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

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

Recovery:

1. Navigate to **Status & Manage** > **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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

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

Recovery:

1. 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:
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. This event is potentially caused by the DSR 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
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

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
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:003

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes of this event are:
   - DSR 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
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:004

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. 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
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8000 - 102 - MpEvFsmException_PeerDisconnected

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:102

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. No action required.

8000 - 103 - MpEvFsmException_PeerUnreachable

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:103

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. 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
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:104

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes for this event are:
   - The peer is misconfigured.
   - The host is misconfigured.

8000 - 105 - MpEvFsmException_CerTimeout

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:105

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. No action required.

8000 - 106 - MpEvFsmException_AuthenticationFailure

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:106

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery

1. Potential causes for this event are:
   - The peer is misconfigured.
   - The host is misconfigured.

8000 - 201 - MpEvFsmException_UdpSocketLimit

Event Type
DIAM

Description
DA-MP connection FSM exception.

Severity
Info

Instance
<DA-MP Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvFsmException

Recovery:

1. The DSR supports to a preconfigured maximum number of open UDP sockets (the maximum number of open UDP sockets can be accessed via **Diameter** > **Configuration** > **System Options** > **Maximum Open RADIUS UDP sockets per DA-MP**). 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
DA-MP exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
None

OID
eagleXgDiameterMpEvException

Recovery

1. Bounce one or more floating connections to force their migration to another DA-MP with available capacity.

8002 - MpEvRxException

8002 - 001 - MpEvRxException_DiamMsgPoolCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. Potential causes of this event are:
   - One or more DA-MPs are unavailable and traffic has been distributed to the remaining DA-MPs.
   - One or more peers are generating more traffic than is nominally expected.
   - There are an insufficient number of DA-MPs provisioned.
   - One or more peers are answering slowly, causing a backlog of pending transactions.

8002 - 002 - MpEvRxException_MaxMpsExceeded

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:002

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is potentially caused when a peer is generating more traffic than is nominally expected.

8002 - 003 - MpEvRxException_CpuCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:003

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. 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
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:004

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 005 - MpEvRxException_DstMpUnknown

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:005

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 006 - MpEvRxException_DstMpCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:006

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. 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
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:007

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 008 - MpEvRxException_DrlAnsQueueCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:008

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 009 - MpEvRxException_ComAgentCongested

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:009

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.

8002 - 201 - MpEvRxException_MsgMalformed

Event Type
DIAM

Description
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:201

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. 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
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

Recovery

1. 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

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** > **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** > **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** > **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
DA-MP ingress message processing exception.

Severity
Info

Instance
<DA-MP Name>:204

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvRxException

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** > **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** > **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** > **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.

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

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

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** > **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** > **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** > **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

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

Recovery:

1. 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
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:001

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery

1. No action required.

8003 - 101 - MpEvTxException_DclTxTaskQueueCongested

Event Type
DIAM

Description
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:101

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery

1. 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

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
DA-MP egress message processing exception.

Severity
Info

Instance
<DA-MP Name>:202

HA Score
Normal

Throttle Seconds
10

OID
eagleXgDiameterMpEvTxException

Recovery:

1. Adjust the Diameter **Pending Answer Timer** option of the associated Transaction 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. MP server status can be monitored from the **Status & Manage** > **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** > **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** > **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.

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

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** > **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** > **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** > **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

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** > **Configuration** > **Connections** screen, which indicates the associated Local Node.
3. Access the Local Node screen via **Diameter** > **Configuration** > **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

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

Recovery

1. 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

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

Recovery

1. 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

Recovery

1. 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

Recovery

1. This event is potentially caused by the DSR 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

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

Recovery

1. Potential causes for this event are:
   - DSR 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery:

1. 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

Recovery:

1. 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

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.

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

Recovery:

1. The peer is responding slowly, network latency is high, or the ETR timer is configured too small. Adjust the Diameter **Pending Answer Timer** option of the associated Transaction 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

Recovery:

1. 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

Recovery:

1. 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

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 DSR and on the RADIUS peer. The shared secret configuration set associated with the transport connection on the DSR can be accessed via **Diameter** > **Configuration** > **Connections**.
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

Recovery:

1. 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

Recovery:

1. 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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery:

1. 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

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.

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

Recovery:

1. This event is unexpected. It is recommended to contact My Oracle Support for assistance.
2. This event is typically generated when the DSR 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. The message authenticator configuration set can be identified by accessing the connection screen via **Diameter** > **Configuration** > **Connections**.

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

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

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

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

Recovery:

1. 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

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** option in System Options to ensure it is sufficient for the offered traffic load.

8010 - MpIngressDrop

Alarm Group
DIAM

Description
An ingress message is discarded or rejected.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpIngressDrop

Recovery

1. Potential causes of this alarm are:
   - One or more DA-MPs are unavailable and traffic has been distributed to the remaining DA-MPs.
   - One or more peers are generating more traffic than is nominally expected.
   - There are an insufficient number of DA-MPs 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

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
DA-MP ingress NGN-PS message rate threshold crossed.

Severity
Major

Instance
MpRxNgnPsOfferedRate, DIAM

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRxNgnPsOfferedRateNotify

Recovery

1. Check for one or more DA-MPs is unavailable and traffic has been distributed to the remaining DA-MPs.
2. Check for one or more peers is generating more traffic than is nominally expected.
3. Check for an insufficient number of DA-MPs provisioned.
4. This alarm clears when the treshold crossing abates.

8013 - MpNgnPsStateMismatch

Alarm Group
DIAM

Description
DA-MP NGN-PS administrative and operational state mismatch.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpNgnPsStateMismatch

Recovery

1. This alarm is potentially caused when a DA-MP 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
DA-MP NGN-PS message discarded or rejected.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpNgnPsDrop

Recovery

1. 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 DSR lacking NGN-PS support.

Severity
Major

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterNgnPsMsgMisrouted

Recovery

1. Potential causes of this alarm are:
   - Routing configuration is incorrect.
   - Peer **DSR** has not yet been upgraded.
   - Peer **DSR** 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

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
DA-MP Task CPU utilization threshold crossed

Severity
Minor, Major, Critical

Instance
Task Name

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpTaskCpuCongested

Recovery

1. 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 DSR lacking 16 priority support

Severity
Major

Instance
<Connection Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterP16MsgMisrouted

Recovery

1. Potential causes of this alarm are:
   - Peer DSR has not yet been upgraded.
   - Peer DSR has not yet operationally enabled 16 priority support.

8019 - MpAnswerPriorityModeMismatch

Alarm Group
DIAM

Description
DA-MP Answer Priority Mode administrative and operational state mismatch.

Severity
Major

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
30

OID
eagleXgDiameterMpAnswerPriorityModeMismatch

Recovery

1. Potential causes of this alarm are:
   - A DA-MP restart is required.

8020 - MpRoutingThreadPoolStateMismatch

Alarm Group
DIAM

Description
Routing Thread Pool administrative and operational state mismatch.

Severity
Minor

Instance
<DA-MP Name>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
eagleXgDiameterMpRoutingThreadPoolStateMismatch

Recovery

1. This alarm is potentially caused when a DA-MP 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

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

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

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** > **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** > **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** > **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

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

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** > **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** > **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** > **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

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

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** > **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** > **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** > **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

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

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

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

Recovery:

1. 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

Recovery:

1. Modify one of the Peer Routing Rule Priorities using the **Diameter > Configuration > Peer Routing Rules** GUI page.

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

Recovery:

1. 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

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 by navigating to **Diameter > Configuration > 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

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. The list of Application IDs that the peer supports on each connection can be viewed as follows:

a. Navigate to **Diameter > Maintenance > Connections**.

b. Locate the relevant Peer Node and check the supported Application IDs.

2. If Application IDs are not the same for each connection (but should be) the Application ID for any connection can be refreshed by:

   a. Navigate to **Diameter > Maintenance > Connections**.

   b. Locate the relevant Connection.

   c. Disable the Connection.

   d. Enable the Connection.

3. 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

Recovery:

1. If this event is occurring frequently, the transaction timers may be set too low. Navigate to **Diameter > Configuration > Pending Answer Timers** to view and/or modify the Pending Answer Timer, Transaction Request Lifetime, peer node settings.

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

Recovery:

1. It is recommended that application routing rules be unique for the same type of messages to avoid unexpected routing results. Peer routing rule priorities can be modified using **Diameter** > **Configuration** > **Application Route Tables** page.
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 DA-MP server, care must be taken to prevent excessive event generation with these resources.

OID:
eagleXgDiameterSpecifiedDasRouteListNotProvisionedNotify

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

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 DA-MP server, care must be taken to prevent excessive event generation with these resources.

OID:
eagleXgDiameterNumberOfRetransmitsExceededToDasNotify

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

Recovery:

1. 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** > **Configuration** > **System Options**.

When this alarm is generated, the system clears all individual peer node alarms (alarm 22051) for the peer node. These alarms can be viewed in **Alarms & Events** > **View Active**.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterPeerNodeUnavailableThresholdReachedNotify

Recovery:

1. Navigate to **Diameter** > **Maintenance** > **Peer Nodes** to monitor 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.

Note: The alarm thresholds are configurable using the Alarm Threshold Options tab on **Diameter** > **Configuration** > **System Options**.

Severity:
Critical

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterRouteListUnavailableThresholdReachedNotify

Recovery:

1. Use **Main Menu** > **Diameter** > **Maintenance** > **Route Lists** 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 DA-MP 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

Recovery:

1. No action necessary.

22019 - Maintenance Leader HA Notification to go OOS

Alarm Group:
DIAM

Description:
This alarm occurs when a DA-MP 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

Recovery:

1. 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:
<DA-MP>

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

Recovery:

1. Verify the size of the Request and Answer messages and see it exceeds the system set message size.

   Use **Main** > **Diameter** > **Configuration** > **Route Lists** to correct provisioning.

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

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

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 under **Diameter** > **Maintenance** > **Connections**.
- 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

Recovery:

1. Confirm a connection is provisioned for the peer node.
   - Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
   - 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.

     From the active SO GUI, navigate to **Diameter** > **Maintenance** > **Peer Nodes**. View the Transaction Configuration Set of the peer node.

     If the peer node has a corresponding Transaction Configuration Set setting, then navigate to **Diameter** > **Configuration** > **Configuration Sets** > **Transaction Configuration Sets** and 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

Recovery:

1. Peer status can be monitored from **Diameter** > **Maintenance** > **Peer Nodes**.
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 configure from **Diameter** > **Maintenance** > **Peer Nodes**.
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

Recovery:

1. Route List status can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
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

Recovery:

1. Verify Route List status and configured minimum capacity from **Diameter** > **Maintenance** > **Route Lists**.
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

Recovery:

1. Route List status and configured minimum capacity can be monitored from **Diameter** > **Maintenance** > **Route Lists**.
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

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 via the following GUI menu: **Diameter** > **Maintenance** > **Connections**
   b. Wait for this alarm to clear.
   c. Disable the connection via the following GUI menu: **Diameter** > **Maintenance** > **Connections**

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 via the following **Diameter** > **Maintenance** > **Connections**
   b. Wait for this alarm to clear.
   c. Enable the connection via the following GUI menu: **Diameter** > **Maintenance** > **Connections**
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

Recovery:

1. Check the configuration in **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Diameter** > **Maintenance** > **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

Recovery:

1. Check the configuration in **Diameter** > **Configuration** > **Egress Throttle Groups** to determine if the Maximum Configured rate is too low.
2. Check the Egress Message Rate at **Diameter** > **Maintenance** > **Egress Throttle Groups** and **Main Menu** > **Diameter** > **Maintenance** > **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

Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Diameter** > **Configuration** > **Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Diameter** > **Maintenance** > **Egress Throttle Groups** and/or **Diameter** > **Maintenance** > **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

Recovery:

1. The Maximum Configured rate may be too low. Check the configuration in **Diameter** > **Configuration** > **Egress Throttle Groups**
2. The sending Peers/Connections are offering too much traffic. Check the EMR rate at **Diameter** > **Maintenance** > **Egress Throttle Groups** and/or **Diameter** > **Maintenance** > **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

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** > **Maintenance**.
2. Verify ComAgent links are established between DA-MPs under **Communication Agent** > **Maintenance**
3. Verify the No-MP Leader condition in **Diameter** > **Maintenance** > **DA-MPs** > **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

Recovery:

1. Ensure that all MME/SGSN hostnames to be hidden are present in the MME/SGSN Configuration Set.
2. If any DSR Applications are activated on DSR, 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 DSR has exceeded its max limits.

Severity:
Info

Instance:
<TransConnName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDiameterMaxMsgSizeLimitExceededNotify

Recovery:

1. 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 DSR 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

Recovery:

1. Examine the DA-MP 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

Recovery:

1. Examine the DA-MP 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

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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery

1. 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

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** > **Maintenance**.
2. Verify ComAgent links are established between DA-MPs under **Communication Agent** > **Maintenance**
3. Verify the No-MP Leader condition in **Diameter** > **Maintenance** > **DA-MPs** > **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

Recovery

1. 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 DSR Application is disabled or not available.

Severity:
Major

Instance:
<DSR Application Name>

HA Score:
Normal

Auto Clear Seconds:
0

OID:
eagleXgDiameterArtMatchAppUnavailableNotify

Recovery:

1. Check the Application Status by navigating to **Diameter** > **Maintenance** > **Applications** and Enable the application if the Admin State of the DSR application is Disabled for a particular DA-MP(s) which raised the alarm.
2. If the Application is Enabled for a particular DA-MP, 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

Recovery

1. 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 DA-MP 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 DSR process is stopped or restarted.

OID:
eagleXgDiameterMpExcessiveRequestRerouteNotify

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 DSR 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 (**Diameter** > **Maintenance** > **Peer Node**).

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 (**Diameter** > **Maintenance** > **Peer Node**).

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

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

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 DSR 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

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

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

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

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: DA-MP Ingress MessageRate Control

Alarm Group:
DIAM

Description:
An ingress message is discarded due to connection (or DA-MP) ingress message rate exceeding connection (or DA-MP) maximum ingress MPS. (Deprecated by DSR 7.2 See 8010 - MpIngressDrop).

Severity:
Major

Instance:
<MPHostName>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIngressMessageDiscardedAlarmNotify

Recovery:

1. The ingress MPS on the DA-MP is exceeding the MP Maximum ingress MPS. Maybe one or more DA-MPs is unavailable and traffic has been distributed to the remaining DA-MPs.
2. See if one or more peers are generating more traffic than is normally expected.
3. Make sure a sufficient number of DA-MPs is provisioned.
4. If the problem persists, it is recommended to contact My Oracle Support.

22200 - MP CPU Congested

Alarm Group:
ExgStack

Description:
DA-MP 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 DA-MP has failed, causing the redistribution of traffic to the remaining DA-MPs

Severity:
Minor, Major, Critical, Warning

Instance
NA

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpCpuCongestedNotify

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 from **Status & Manage** > **Server**.

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** > **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. The ingress traffic rate of each MP can be monitored from the **Status & Manage** > **KPIs** page. 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 from **Alarms & Events**.
5. If the problem persists, it is recommended to contact My Oracle Support.

22201 - MpRxAllRate

Alarm Group:
DIAM

Description:
DA-MP ingress message rate threshold crossed.

Severity:
Minor, Major, Critical

Instance:
MpRxAllRate, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpRxAllRateNotify

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** > **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** > **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** > **KPIs** page. 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:
DA-MP Diameter message pool utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
MpDiamMsgPool, DIAM

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMpDiamMsgPoolCongestedNotify

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** > **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** > **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** > **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.

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

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** > **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** > **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** > **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 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.
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

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** > **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** > **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** > **KPIs** page. 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. The alarm log should be examined from the **Alarms & Events** page.
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

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** > **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** > **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** > **KPIs** page. 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. The alarm log should be examined from the **Alarms & Events** page.
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

Recovery:

1. An excessive amount of Request message rerouting may have been triggered by either connection failures or Answer time-outs. The status of connections should be examined from the **Diameter** > **Maintenance** > **Connections** page.

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. The alarm log should be examined using the **Alarms & Events** page.
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:
<DA-MP Name>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDclTxTaskQueueCongested

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

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

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** > **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** > **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** > **KPIs** page. 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. The alarm log should be examined using the **Alarms & Events** page.

5. If the problem persists, contact My Oracle Support.

22214 - Message Copy Queue Utilization

Alarm Group:
DIAM

Description:
The DA-MP'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

Recovery:

1. Reduce traffic to the MP.
2. Verify that no network issues exist between the DA-MP 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

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.

   MP server status can be monitored from **Status & Manage** > **Server Status**.

2. The mis-configuration of Diameter peers may result in too much traffic being distributed to the MP.

   The routing mps rate of each MP can be monitored from **Status & Manage** > **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.

   The routing mps rate of each MP can be monitored from **Status & Manage** > **KPIs**. 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

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** > **Server Status**.

2. The misconfiguration of Pending Answer Timer assignment may result in excessive traffic being assigned to the Long Timeout PTR buffer Pool. View the Pending Answer Timer values via **Diameter** > **Configuration** > **Pending Answer Timers**. Examine the Pending Answer Timers assignment via the **Diameter** > **Configuration** > **Application Ids and Diameter** > **Configuration** > **Peer Nodes**.
3. The misconfiguration 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** > **KPIs**. 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. Monitor the ingress traffic rate of each MP from **Status & Manage** > **KPIs**. 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 from **Alarms & Events**.
6. If the problem persists, it is recommended to contact My Oracle Support.

22223 - DA-MP Memory Utilization Threshold Crossed

Alarm Group:
DIAM

Description:
DA-MP memory utilization threshold crossed.

Severity:
Minor, Major, Critical

Instance:
System.RAM_UtilPct, DSR

HA Score:
Normal

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

OID:
eagleXgDiameterMpMemCongestedNotify

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 DA-MPs.
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 DSR-wide engineering attributes associated with average hold time, defined in the DA-MP profile assigned to the DA- MP 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 DA-MP 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 by navigating to **Status & Manage** > **Server**.

Severity:
Minor, Major, Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterAvgHoldTimeLimitExceededNotify

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 DSR sending requests to the upstream peers and receiving answers for the requests.
   - Confirm the peer node(s) or DSR 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 on **Diameter Common** > **MPs** > **Profiles**:

   - 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 DSR has exceeded its configured limits.

The alarm is generated when the measurement RxAvgMsgSize reaches the DSR-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 DSR.

This alarm indicates DSR 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

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 DSR to that message.
2. The alarm thresholds are configurable on **Diameter Common** > **MPs** > **Profiles**:
   - 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

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** > **Configuration** > **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** > **Configuration** > **System Options**.

Instance:
<NetworkElement>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterIPFEConnUnavailableThresholdReachedNotify

Recovery:

1. Navigate to **Diameter** > **Maintenance** > **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 DA-MP.

Note: The alarm thresholds are configurable using the Alarm Threshold Options tab on **Diameter** > **Configuration** > **System Options**.

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** > **Configuration** > **System Options**.

Instance:
<DA-MP-Hostname>

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterConnUnavailableThresholdReachedNotify

Recovery:

1. Navigate to **Diameter** > **Maintenance** > **Connection** to monitor 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. Navigate to **Diameter** > **Configuration** > **System Options** to check the Alarm Threshold Options setting. Modify the value 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 DA-MP RT-DBs has overrun. The DA-MP'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

Recovery:

1. 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

Recovery:

1. It is recommended to contact My Oracle Support.

22950 - Connection Status Inconsistency Exists

Alarm Group:
DIAM

Description:
Diameter Connection status inconsistencies exist among the DA-MPs in the DSR 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

Recovery:

1. No action necessary.

Note: DA-**MP**'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

Recovery:

1. From the DSR OAM GUI, navigate to **Diameter Common** > **MPs** > **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 DA-MP is brought into service and a DA-MP configured DiamaterMaxMessageSize in DpiOption table value is greater than 16KB, but the available memory on DA-MP is less than 48GB.

Severity:
Critical

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterInsufficientAvailMemNotify

Recovery:

1. Make additional memory available on the DA-MP 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

Recovery

1. Navigate to the Signaling Firewall page (**Diameter** > **Maintenance** > **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

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** > **Maintenance** > **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

Recovery

1. 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

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

Recovery

1. If the problem persists, it is recommended to contact My Oracle Support for assistance.

25612 - DSR ping failed

Alarm Group
DIAM

Description
Connection was rejected due to the DA-MP exceeding its connection or ingress MPS capacity

Severity
Major

Instance
pingAllLivePeers

HA Score
Normal

Auto Clear Seconds
N/A

OID
eagleXgDiameterPingAllLivePeerErrorNotify

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.

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

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 SOAM Server Group Designation

Alarm Group
DIAM

Description
Invalid Internal SOAM 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

Recovery

1. 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

Recovery:

1. 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

Recovery:

1. The DSR **Relay Agent** forwarded a Request message to the address resolution application which contained an unrecognized Diameter Application ID in the

header. Either a DSR **Relay Agent** application routing rule is mis-provisioned or the Application ID is not provisioned in the RBAR routing configuration.

2. View the currently provisioned Diameter Application IDs by selecting **RBAR** > **Configuration** > **Applications**.
3. View the currently provisioned Application Routing Rules by selecting **Diameter** > **Configuration** > **Application Route Tables**.

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

Recovery:

1. The order pair (Application ID, Command Code) is not provisioned in the Address Resolutions routing configuration.
2. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

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

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. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

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

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. View the currently provisioned Application IDs and Command Codes by selecting **RBAR** > **Configuration** > **Address Resolutions**.

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

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** > **Configuration** > **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 DSR 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

Recovery:

1. 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

Recovery:

1. If this problem occurs, it is recommended to contact My Oracle Support.

Generic Application Alarms and Events (22500-22599)

Note: These alarms are generic across the various DSR applications with some details varying depending on the application generating the alarm.

22500 - DSR Application Unavailable

Alarm Group:
APPL

Description:
DSR application is unable to process any messages because it is unavailable.

Severity:
Critical

Instance:
<DSR Application Name>

> **Note:** The value for DSR Application Name varies depending on the DSR application generating the alarm (DCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationUnavailableNotify

Recovery:

1. Display and monitor the DSR application status by navigating to **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify the Admin State is set as expected.
2. A DSR 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. A DCA application that defines a logical-to-physical U-SBR DB mapping becomes unavailable if the U-SBR DBs are not enabled or their sub-resources are unreachable. The status of the U-SBR DBs can be monitored from **SBR** > **Maintenance** > **SBR DB Status.**

   > **Note:** A DCA application can also become unavailable if there are no production or trial versions available. Trial DA-MPs run the production version if a trial version is not available. Non-Trial DA-MPs run only the production version.

4. Check the Event History logs for additional DIAM events or alarms for this MP server.
5. If the problem persists, it is recommended to contact My Oracle Support.

22501 - DSR Application Degraded

Alarm Group:
APPL

Description:
Unable to forward requests to the DSR application because it is degraded.

Severity:
Major

Instance:
<DSR Application Name>

> **Note:** The value for DSR Application Name varies depending on the DSR application generating the alarm (DCA, PCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationDegradedNotify

Recovery:

1. Display and monitor the DSR application status by navigating to **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify the Admin State is set as expected.
2. A DSR application becomes degraded when the DSR application becomes congested, if enabled.

> **Note:** This alarm is NOT raised when the DSR application is shutting down gracefully or application is in the disabled state. Only the DSR 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 - DSR Application Request Message Queue Utilization

Alarm Group:
APPL

Description:
The DSR Application Request Message Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
<Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm varies (RxPdraRequestMsgQueue, RxCpaRequestMsgQueue, or RxDcaRequestMsgQueue[<DcaDalId.dalId>], for example) depending on which DSR application generates the alarm (CPA, DCA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name will vary depending on the DSR application generating the alarm (CPA, DCA, FABR, PCA, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationRequestQueueUtilNotify

Recovery:

1. Display and monitor the DSR application status by selecting **Diameter** > **Maintenance** > **Applications** in the SO GUI. Verify the Admin State is set as expected.

   The DSR 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 DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Route Tables** in the SO GUI.

3. If no additional congestion alarms are asserted, the DSR application task might be experiencing a problem that is preventing it from processing messages from its Request Message Queue. Examine the Alarm log in **Alarms & Events** on the active SOAM server.

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

22503 - DSR Application Answer Message Queue Utilization

Alarm Group:
APPL

Description:
The DSR Application Answer Message Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
<Metric ID>, <DSR Application Name>

Note: The value for Metric ID for this alarm varies (RxPdraAnswerMsgQueue, RxCpaAnswerMsgQueueor, or RxDcaRequestMsgQueue[<DcaDalId.dalId>], for example) depending on which DSR application generates the alarm (CPA, DCA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for the DSR Application Name varies depending on the DSR application generating the alarm (CPA, PCA, FABR, Policy DRA, RBAR, DCA, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationAnswerQueueUtilNotify

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Route Tables** in the SO GUI.
2. If no additional congestion alarms are asserted, the DSR application task might be experiencing a problem that is preventing it from processing message from its Answer Message Queue. Examine the Alarm log in **Alarms & Events** on the active SOAM server.
3. If the problem persists, it is recommended to contact My Oracle Support.

22504 - DSR Application Ingress Message Rate

Alarm Group:
APPL

Description:
The ingress message rate for the DSR application is exceeding its engineered traffic handling capacity.

Severity:
Minor, Major, Critical

Instance:
<Metric ID>, <DSR Application Name>

Note: The value for metric ID for this alarm varies (RxPdraMsgRate, RxCpaMsgRate, for example) depending on which DSR application generates the alarm (CPA, FABR, Policy DRA, RBAR, etc.). Use the ID that corresponds to the specific DSR application in use.

Note: The value for DSR Application Name varies depending on the DSR application generating the alarm (CPA, PCA, FABR, Policy DRA, RBAR, etc.). Use the name that corresponds to the specific DSR application in use.

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationIngressMsgRateNotify

Recovery:

1. Application routing may be mis-configured and is sending too much traffic to the DSR application. Verify the configuration by selecting **Diameter** > **Configuration** > **Application Route Tables** in the SO GUI.
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** > **KPIs**.
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 - DSR Application Enabled

Event Type:
APPL

Description:
DSR Application Admin state was changed to 'enabled'.

Severity:
Info

Instance:
<DSR Application Name>, the DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationEnabledNotify

Recovery:

1. No action required.

22521 - DSR Application Disabled

Event Type:
APPL

Description:
DSR Application Admin state was changed to 'disabled'.

Severity:
Info

Instance:
<DSR Application Name>, the DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score:
Normal

Throttle Seconds:
0 (zero)

OID:
eagleXgDiameterDsrApplicationDisabledNotify

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. The currently provisioned Application Routing Rules can be viewed using **Diameter** > **Configuration** > **Application Route Tables**.
2. The currently provisioned Diameter Application IDs can be viewed in the **FABR** > **Configuration** > **Applications Configuration**.
3. It is recomended 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

Recovery:

1. The currently provisioned Application Routing Rules can be viewed using **Diameter** > **Configuration** > **Application Route Tables**.

2. The currently provisioned Diameter Application IDs can be viewed in the **FABR** > **Configuration** > **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

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** > **Configuration** > **Address Resolutions**.
2. The currently provisioned Application Routing Rules can be viewed using **Diameter** > **Configuration** > **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

Recovery:

1. If this event is considered abnormal, then navigate to **FABR** > **Configuration** > **Address Resolutions** to validate which AVPs are configured for routing with the Application ID and Command Code.
2. Navigate to **Diameter** > **Configuration** > **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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

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

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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. Check the P-DRA GUI at **Policy DRA** > **Configuration** > **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

Recovery:

1. If the event was generated for a Diameter message being discarded due to congestion, refer to the Recovery steps for Alarm 22504 - DSR 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

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** > **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

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** > **Configuration** > **Online Charging DRA** > **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** > **Configuration** > **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** > **Configuration** > **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** > **Maintenance** > **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** > **Maintenance** > **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

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** > **Configuration** > **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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. Check the Policy and Charging GUI Main Menu **Policy and Charging** > **Configuration** > **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** > **Configuration** > **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

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)

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** > **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** > **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** > **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)

Recovery:

1. Adjust the alarm threshold parameters. Verify the configuration by navigating to the Congestion Options on **Policy DRA** > **Configuration** > **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** > **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)

Recovery:

1. At the NOAM, navigate to the SBR Database Status screen at **Policy and Charging** > **Maintenance** > **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** > **Resource Domains**
   - **Configuration** > **Places**
   - **Configuration** > **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** > **Maintenance** > **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)

Recovery:

1. At the NOAM, navigate to the SBR Database Status screen at **Policy and Charging** > **Maintenance** > **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** > **Resource Domains**
- **Configuration** > **Places**
- **Configuration** > **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** > **Maintenance** > **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

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

Recovery:

1. Application Routing might be mis-configured and is sending too much traffic to the DSR Application. Verify the configuration by selecting **Diameter** > **Configuration** > **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** > **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

Recovery:

1. 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

Recovery:

1. 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

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** > **Configuration** > **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

Recovery:

1. Check the NOAM GUI at **Policy and Charging** > **Configuration** > **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)

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** > **Configuration** > **Policy DRA** > **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** > **Configuration** > **Policy DRA** > **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** > **Configuration** > **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** > **Configuration** > **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** > **Configuration** > **Online Charging DRA** > **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** > **Configuration** > **Online Charging DRA** > **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

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

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

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)

Recovery:

1. From the NOAM GUI at **Policy and Charging** > **Maintenance** > **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** > **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

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

Recovery:

1. 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)

Recovery:

1. Make note of all **Status & Manage** > **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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery

1. 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

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** > **Configuration** > **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** > **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

Recovery:

1. 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.

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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** > **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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. Verify the MP operational status of the DA-MP from the **Diameter** > **Maintenance** > **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** > **Maintenance** > **DA-MP** active SOAM screen.
   c. Verify ComAgent inter-MP connections (auto) are in the InService state on the **Communication Agent** > **Maintenance** > **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

Recovery:

1. Verify the MP operational status of the DA-MP from the **Diameter** > **Maintenance** > **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** > **Maintenance** > **DA-MP** active SOAM screen.
   c. Verify ComAgent inter-MP connections (auto) are in the InService state on the **Communication Agent** > **Maintenance** > **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

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

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

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

Recovery:

1. 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

Recovery:

1. 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

Recovery:

1. No action is required. This event is used for command-line tool errors only.

31001 - S/W status

Alarm Group:
SW

Description:
Program status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolSwStatusNotify

Recovery:

1. No action required.

31002 - Process watchdog failure

Alarm Group:
SW

Description:
Process watchdog timed out.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolProcWatchdogFailureNotify

Recovery:

1. Alarm indicates a stuck process was automatically recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs ,and it is recommended to contact My Oracle Support.

31003 - Tab thread watchdog failure

Alarm Group:
SW

Description:
Tab thread watchdog timed out

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolThreadWatchdogFailureNotify

Recovery:

1. Alarm indicates 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 s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbReplicationFaultNotify

Recovery:

1. Export event history for the given server and inetsync task.

2. It is recommended to contact My Oracle Support.

31101 - Database replication to slave failure

Alarm Group:
REPL

Description:
Database replication to a slave database has failed. This alarm is generated when:

- The replication master finds the replication link is disconnected from the slave.
- The replication master's link to the replication slave is OOS, or the replication master cannot get the slave's correct HA state because of a failure to communicate.
- The replication mode is relayed in a cluster and either:
  - No nodes are active in cluster, or
  - None of the nodes in cluster are getting replication data.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepToSlaveFailureNotify

Recovery:

1. Verify the path for all services on a node by typing `path.test –a <toNode>` in a command interface to test the paths for all services.
2. Use the path test command to test the communication between nodes by typing `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

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 DB.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepUpdateFaultNotify

Recovery:

1. This alarm indicates a transient error occurred within the replication subsystem, but the system has recovered, so no additional steps are needed.
2. If the problem persists, collect savelogs, and it is recommended to contact My Oracle Support.

31104 - DB Replication latency over threshold

Alarm Group:
REPL

Description:
Database replication latency has exceeded thresholds

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepLatencyNotify

Recovery:

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, it is recommended to contact My Oracle Support.

31105 - Database merge fault

Alarm Group:
SW

Description:
The database merge process (inetmerge) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeFaultNotify

Recovery:

1. This alarm indicates a transient error occurred within the merging subsystem, but the system has recovered, so no additional steps are needed.
2. If the problem persists, collect savelogs, and it is recommended to contact My Oracle Support.

31106 - Database merge to parent failure

Alarm Group:
COLL

Description:
Database merging to the parent Merge Node has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolDbMergeToParentFailureNotify

Recovery:

1. This alarm indicates the merging subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact My Oracle Support.

31107 - Database merge from child failure

Alarm Group:
COLL

Description:
Database merging from a child Source Node has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeFromChildFailureNotify

Recovery:

1. This alarm indicates the merging subsystem is unable to contact a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact My Oracle Support.

31108 - Database merge latency over threshold

Alarm Group:
COLL

Description:
Database Merge latency has exceeded thresholds

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeLatencyNotify

Recovery:

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, it is recommended to contact My Oracle Support.

31109 - Topology config error

Alarm Group:
DB

Description:
Topology is configured incorrectly

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolTopErrorNotify

Recovery:

1. This alarm may occur during initial installation and configuration of a server. No action is necessary at that time.
2. If this alarm occurs after successful initial installation and configuration of a server, it is recommended to contact My Oracle Support.

31110 - Database audit fault

Alarm Group:
SW

Description:
The Database service process (idbsvc) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbAuditFaultNotify

Recovery:

1. Alarm indicates an error occurred within the database audit system, but the system has recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs, and it is recommended to contact My Oracle Support.

31111 - Database merge audit in progress

Alarm Group:
COLL

Description:
Database Merge Audit between mate nodes in progress

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMergeAuditNotify

Recovery:

1. No action required.

31112 - DB replication update log transfer timed out

Alarm Group:
REPL

Description:
DB Replicated data may not have transferred in the time allotted.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
30

OID:
comcolDbRepUpLogTransTimeoutNotify

Recovery:

1. No action required.
2. It is recommended to contact My Oracle Support if this occurs frequently.

31113 - DB replication manually disabled

Alarm Group:
REPL

Description:
DB Replication Manually Disabled

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolDbReplicationManuallyDisabledNotify

Recovery:

1. No action required.

31114 - DB replication over SOAP has failed

Alarm Group:
REPL

Description:
Database replication of configuration data via **SOAP** has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
3600

OID:
comcolDbReplicationSoapFaultNotify

Recovery:

1. This alarm indicates a SOAP subsystem is unable to connect to a server, due to networking issues or because the server is not available. Investigate the status of the server and verify network connectivity.
2. If no issues with network connectivity or the server are found and the problem persists, it is recommended to contact My Oracle Support.

31115 - Database service fault

Alarm Group:
SW

Description:
The Database service process (idbsvc) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbServiceFaultNotify

Recovery:

1. Alarm indicates an error occurred within the database disk service subsystem, but the system has recovered, so no additional steps are needed.
2. If this problem persists, collect savelogs, and it is recommended to contact My Oracle Support.

31116 - Excessive shared memory

Alarm Group:
MEM

Description:
The amount of shared memory consumed exceeds configured thresholds.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolExcessiveSharedMemoryConsumptionNotify

Recovery:

1. This alarm indicates that a server has exceeded the engineered limit for shared memory usage and there is a risk that application software will fail. Because there is no automatic recovery for this condition, it is recommended to contact My Oracle Support.

31117 - Low disk free

Alarm Group:
DISK

Description:
The amount of free disk is below configured thresholds

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolLowDiskFreeNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, it is recommended to contact My Oracle Support.

31118 - Database disk store fault

Alarm Group:
DISK

Description:
Writing the database to disk failed

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbDiskStoreFaultNotify

Recovery:

1. Remove unnecessary or temporary files from partitions.
2. If there are no files known to be unneeded, it is recommended to contact My Oracle Support.

31119 - Database updatelog overrun

Alarm Group:
DB

Description:
The Database update log was overrun increasing risk of data loss

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbUpdateLogOverrunNotify

Recovery:

1. This alarm indicates a replication audit transfer took too long to complete and the incoming update rate exceeded the engineered size of the update log. The system will automatically retry the audit, and if successful, the alarm will clear and no further recovery steps are needed.
2. If the alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31120 - Database updatelog write fault

Alarm Group:
DB

Description:
A Database change cannot be stored in the updatelog

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbUpdateLogWriteFaultNotify

Recovery:

1. This alarm indicates an error has occurred within the database update log subsystem, but the system has recovered.
2. If the alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31121 - Low disk free early warning

Alarm Group:
DISK

Description:
The amount of free disk is below configured early warning thresholds

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolLowDiskFreeEarlyWarningNotify

Recovery:

1. Remove unnecessary or temporary files from partitions that are greater than 80% full.
2. If there are no files known to be unneeded, it is recommended to contact My Oracle Support.

31122 - Excessive shared memory early warning

Alarm Group:
MEM

Description:
The amount of shared memory consumed exceeds configured early warning thresholds

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolExcessiveShMemConsumptionEarlyWarnNotify

Recovery:

1. This alarm indicates that a server is close to exceeding the engineered limit for shared memory usage and the application software is at risk to fail. There is no automatic recovery or recovery steps.
2. It is recommended to contact My Oracle Support.

31123 - Database replication audit command complete

Alarm Group:
REPL

Description:
ADIC found one or more errors that are not automatically fixable.

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepAuditCmdCompleteNotify

Recovery:

1. No action required.

31124 - ADIC error

Alarm Group:
REPL

Description:
An ADIC detected errors

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepAuditCmdErrNotify

Recovery:

1. It is recommended to contact My Oracle Support.

31125 - Database durability degraded

Alarm Group:
REPL

Description:
Database durability has dropped below configured durability level

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbDurabilityDegradedNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.

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

31126 - Audit blocked

Alarm Group:
REPL

Description:
Site Audit Controls blocked an inter-site replication audit due to the number in progress per configuration.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolAuditBlockedNotify

Recovery:

1. This alarm indicates that WAN network usage has been limited following a site recovery. No recovery action is needed.

31127 - DB Replication Audit Complete

Alarm Group:
REPL

Description:
DB replication audit completed

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbRepAuditCompleteNotify

Recovery:

1. No action required.

31128 - ADIC Found Error

Alarm Group:
REPL

Description:
ADIC found one or more errors that are not automatically fixable.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbADICErrorNotify

Recovery:

1. This alarm indicates a data integrity error was found by the background database audit mechanism, and there is no automatic recovery.
2. It is recommended to contact My Oracle Support.

31129 - ADIC Found Minor Issue

Alarm Group:
REPL

Description:
ADIC found one or more minor issues that can most likely be ignored

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
14400

OID:
comcolDbADICWarn

Recovery:

1. No action required.

31130 - Network health warning

Alarm Group:
NET

Description:
Network health issue detected

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolNetworkHealthWarningNotify

Recovery:

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact My Oracle Support.

31131 - DB Ousted Throttle Behind

Alarm Group:
DB

Description:
DB ousted throttle may be affecting processes.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolOustedThrottleWarnNotify

Recovery:

1. This alarm indicates that a process has failed to release database memory segments which is preventing new replication audits from taking place. There is no automatic recovery for this failure.
2. Run '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

Recovery

1. No action required.

31133 - DB Replication Switchover Exceeds Threshold

Alarm Group
REPL

Description
DB Replication Active to Standby switchover exceeded maximum switchover time.

Severity
Major

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbRepSwitchoverNotify

Recovery

1. If this alarm is raised, it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If the problem persists, it is recommended to contact My Oracle Support.

31134 - DB Site Replication To Slave Failure

Alarm Group
REPL

Description
DB Site replication to a slave DB has failed.

Severity
Minor

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbSiteRepToSlaveFailureNotify

Recovery

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact My Oracle Support.

31135 - DB Site Replication From Master Failure

Alarm Group
REPL

Description
DB Site replication from a master DB has failed.

Severity
Minor

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbSiteRepFromMasterFailureNotify

Recovery

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact My Oracle Support.

31136 - DB Site Replication Precedence Relaxed

Event Type
REPL

Description
Standby Site Database updates are falling behind. Relaxing the replication barrier to allow non-Standby Site Databases to update as fast as possible.

Severity
Info

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Throttle Seconds
150

OID
comcolDbSiteRepPrecRelaxedNotify

Recovery

1. No action required.

31137 - DB Site Replication Latency Over Threshold

Alarm Group
REPL

Description
DB Site Replication latency has exceeded thresholds.

Severity
Major

Instance
Remote Node Name + HA resource name (if Policy 0, no resource name)

HA Score
Normal

Auto Clear Seconds
300

OID
comcolDbSiteRepLatencyNotify

Recovery

1. If this alarm is raised occasionally for short time periods (a couple of minutes or less), it may indicate network congestion or spikes of traffic pushing servers beyond their capacity. Consider re-engineering network capacity or subscriber provisioning.
2. If this alarm does not clear after a couple of minutes, it is recommended to contact My Oracle Support.

31140 - Database perl fault

Alarm Group:
SW

Description:
Perl interface to Database is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbPerlFaultNotify

Recovery:

1. This alarm indicates an error has occurred within a Perl script, but the system has recovered.
2. If the alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31145 - Database SQL fault

Alarm Group:
SW

Description:
SQL interface to Database is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbSQLFaultNotify

Recovery:

1. This alarm indicates an error has occurred within the MySQL subsystem, but the system has recovered.
2. If this alarm occurs frequently, it is recommended to collect savelogs and contact My Oracle Support.

31146 - DB mastership fault

Alarm Group:
SW

Description:
DB replication is impaired due to no mastering process (inetrep/inetrep).

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbMastershipFaultNotify

Recovery:

1. Export event history for the given server.
2. It is recommended to contact My Oracle Support.

31147 - DB upsynclog overrun

Alarm Group:
SW

Description:
UpSyncLog is not big enough for (WAN) replication.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbUpSyncLogOverrunNotify

Recovery:

1. This alarm indicates that an error occurred within the database replication subsystem. A replication audit transfer took too long to complete, and during the audit the incoming update rate exceeded the engineered size of the update log. The replication subsystem will automatically retry the audit, and if successful, the alarm will clear.
2. If the alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31148 - DB lock error detected

Alarm Group:
DB

Description:
The DB service process (idbsvc) has detected an IDB lock-related error caused by another process. The alarm likely indicates a DB lock-related programming error, or it could be a side effect of a process crash.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolDbLockErrorNotify

Recovery:

1. This alarm indicates an error occurred within the database disk service subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

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

Recovery

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

31200 - Process management fault

Alarm Group:
SW

Description:
The process manager (procmgr) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcMgmtFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31201 - Process not running

Alarm Group:
PROC

Description:
A managed process cannot be started or has unexpectedly terminated.

Severity:
Major

Instance:
May include process name

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcNotRunningNotify

Recovery:

1. This alarm indicates a managed cannot be started 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 will no longer manage this process.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcZombieProcessNotify

Recovery:

1. This alarm indicates managed process exited unexpectedly and was unable to be restarted automatically.
2. It is recommended to collect savelogs and contact My Oracle Support.

31206 - Process mgmt monitoring fault

Alarm Group:
SW

Description:
The process manager monitor (pm.watchdog) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcMgmtMonFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31207 - Process resource monitoring fault

Alarm Group:
SW

Description:
The process resource monitor (ProcWatch) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcResourceMonFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process monitoring subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31208 - IP port server fault

Alarm Group:
SW

Description:
The run environment port mapper (re.portmap) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolPortServerFaultNotify

Recovery:

1. This alarm indicates an error occurred within the port mapping subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31209 - Hostname lookup failed

Alarm Group:
SW

Description:
Unable to resolve a hostname specified in the NodeInfo table

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHostLookupFailedNotify

Recovery:

1. This typically indicates a DNS Lookup failure. Verify all server hostnames are correct in the GUI configuration on the server generating the alarm.
2. If the problem persists, it is recommended to contact My Oracle Support.

31213 - Process scheduler fault

Alarm Group:
SW

Description:
The process scheduler (ProcSched/runat) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolProcSchedulerFaultNotify

Recovery:

1. This alarm indicates an error occurred within the process management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31214 - Scheduled process fault

Alarm Group:
PROC

Description:
A scheduled process cannot be executed or abnormally terminated

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolScheduleProcessFaultNotify

Recovery:

1. This alarm indicates that a managed process exited unexpectedly due to a memory fault, but the system has recovered.
2. It is recommended to contact My Oracle Support.

31215 - Process resources exceeded

Alarm Group:
SW

Description:
A process is consuming excessive system resources.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
14400

OID:
comcolProcResourcesExceededFaultNotify

Recovery:

1. This alarm indicates a process has exceeded the engineered limit for heap usage and there is a risk the application software will fail.
2. Because there is no automatic recovery for this condition, it is recommended to contact My Oracle Support.

31216 - SysMetric configuration error

Alarm Group:
SW

Description:
A SysMetric Configuration table contains invalid data

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolSysMetricConfigErrorNotify

Recovery:

1. This alarm indicates a system metric is configured incorrectly.
2. It is recommended to contact My Oracle Support.

31217 - Network Health Warning

Alarm Group
SW

Description
Missed Heartbeats Detected

Severity
Minor

Instance
IP Address

HA Score
Normal

Auto Clear Seconds
300

OID
comcolNetworkHealthWarningNotify

Recovery

1. Check configuration of all servers, and check for connectivity problems between server addresses.
2. If the problem persists, it is recommended to contact My Oracle Support.

31220 - HA configuration monitor fault

Alarm Group:
SW

Description:
The **HA** configuration monitor is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaCfgMonitorFaultNotify

Recovery:

1. It is recommended to contact My Oracle Support.

31221 - HA alarm monitor fault

Alarm Group:
SW

Description:
The high availability alarm monitor is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaAlarmMonitorFaultNotify

Recovery:

1. It is recommended to contact My Oracle Support.

31222 - HA not configured

Alarm Group:
HA

Description:
High availability is disabled due to system configuration.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaNotConfiguredNotify

Recovery:

1. It is recommended to contact My Oracle Support.

31223 - HA Heartbeat transmit failure

Alarm Group:
HA

Description:
The high availability monitor failed to send heartbeat.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaHbTransmitFailureNotify

Recovery:

1. This alarm clears automatically when the server successfully registers for HA heartbeating.
2. If this alarm does not clear after a couple minutes, it is recommended to contact My Oracle Support.

31224 - HA configuration error

Alarm Group:
HA

Description:
High availability configuration error

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaCfgErrorNotify

Recovery:

1. This alarm indicates a platform configuration error in the High Availability or VIP management subsystem.
2. Because there is no automatic recovery for this condition, it is recommended to contact My Oracle Support.

31225 - HA service start failure

Alarm Group:
HA

Description:
The required high availability resource failed to start.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0

OID:
comcolHaSvcStartFailureNotify

Recovery:

1. This alarm clears automatically when the HA daemon 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:
comcolHaAvailDegradedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, it is recommended to contact My Oracle Support.

31227 - HA availability status failed

Alarm Group:
HA

Description:
The high availability status is failed due to raised alarms.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
N/A

OID:
comcolHaAvailFailedNotify

Recovery:

1. View alarms dashboard for other active alarms on this server.
2. Follow corrective actions for each individual alarm on the server to clear them.
3. If the problem persists, 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:
comcolHaStandbyOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored. It clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, it is recommended to look for network connectivity issues and 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 up 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

Recovery:

1. Status message - no action required.

31230 - Recent alarm processing fault

Alarm Group:
SW

Description:
The recent alarm event manager (raclerk) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolRecAlarmEvProcFaultNotify

Recovery:

1. This alarm indicates an error occurred within the alarm management subsystem, but the system has recovered.

2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31231 - Platform alarm agent fault

Alarm Group:
SW

Description:
The platform alarm agent impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolPlatAlarmAgentNotify

Recovery:

1. This alarm indicates an error occurred within the alarm management subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to contact My Oracle Support.

31232 - Late heartbeat warning

Alarm Group:
HA

Description:
High availability server has not received a message on specified path within the configured interval.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaLateHeartbeatWarningNotify

Recovery:

1. No action is required. This is a warning and can be due to transient conditions. If there continues to be no heartbeat from the server, alarm 31228 - HA standby offline occurs.

31233 - HA Path Down

Alarm Group:
HA

Description:
High availability path loss of connectivity

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaPathDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the secondary path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues on the secondary network.
3. It is recommended to contact My Oracle Support.

31234 - Untrusted Time Upon Initialization

Alarm Group:
REPL

Description:
Upon system initialization, the system time is not trusted probably because NTP is misconfigured or the NTP servers are unreachable. There are often accompanying Platform alarms to guide correction. Generally, applications are not started if time is not believed to be correct on start-up. Recovery 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:
comcolUtrustedTimeOnInitNotify

Recovery:

1. Correct NTP configuration.
2. If the problem persists, it is recommended to contact My Oracle Support.

31235 - Untrusted Time After Initialization

Alarm Group:
REPL

Description:
After system initialization, the system time has become untrusted probably because NTP has reconfigured improperly, time has been manually changed, the NTP servers are unreachable, 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 is 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:
comcolUtrustedTimePostInitNotify

Recovery:

1. Correct NTP configuration.

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

31236 - HA Link Down

Alarm Group:
HA

Description:
High availability TCP link is down.

Severity:
Critical

Instance:
Remote node being connected to plus the path identifier

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaLinkDownNotify

Recovery:

1. If loss of communication between the active and standby servers over the specified path is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, it is recommended to look for network connectivity issues on the primary network and/or contact My Oracle Support.

31240 - Measurements collection fault

Alarm Group:
SW

Description:
The measurements collector (statclerk) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolMeasCollectorFaultNotify

Recovery:

1. This alarm indicates that an error within the measurement subsystem has occurred, but that the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to collect savelogs and contact My Oracle Support.

31250 - RE port mapping fault

Alarm Group:
SW

Description:
The IP service port mapper (re.portmap) is impaired by a s/w fault

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolRePortMappingFaultNotify

Recovery:

1. This typically indicates a **DNS** Lookup failure. Verify all server hostnames are correct in the **GUI** configuration on the server generating the alarm.

31260 - SNMP Agent

Alarm Group:
SW

Description:
The SNMP agent (cmsnmpa) is impaired by a s/w fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
eagleXgDsrDbcomcolSnmpAgentNotify

Recovery:

1. This alarm indicates an error occurred within the SNMP subsystem, but the system has recovered.
2. If this alarm occurs repeatedly, it is recommended to collect savelogs and contact My Oracle Support.

31261 - SNMP Configuration Error

Alarm Group
SW

Description
A SNMP configuration error was detected

Severity
Minor

Instance
comcolAlarmSrcNode, comcolAlarmNumber, comcolAlarmInstance, comcolAlarmSeverity, comcolAlarmText, comcolAlarmInfo, comcolAlarmGroup, comcolServerHostname, comcolAlarmSequence, comcolAlarmTimestamp, comcolAlarmEventType, comcolAlarmProbableCause, comcolAlarmAdditionalInfo

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
comcolSnmpConfigNotify

Recovery

1. Export event history for the given server and all processes.
2. It is recommended to contact My Oracle Support for assistance.

31270 - Logging output

Alarm Group:
SW

Description:
Logging output set to Above Normal

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolLoggingOutputNotify

Recovery:

1. Extra diagnostic logs are being collected, potentially degrading system performance. Turn off the debugging log.

31280 - HA Active to Standby transition

Alarm Group:
HA

Description:
HA active to standby activity transition

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolActiveToStandbyTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, it is recommended to contact My Oracle Support.

31281 - HA Standby to Active transition

Alarm Group:
HA

Description:
HA standby to active activity transition

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolStandbyToActiveTransNotify

Recovery:

1. If this alarm occurs during routine maintenance activity, it may be ignored.
2. Otherwise, it is recommended to contact My Oracle Support.

31282 - HA Management Fault

Alarm Group:
HA

Description:
The HA manager (cmha) is impaired by a software fault.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaMgmtFaultNotify

Recovery:

1. This alarm indicates an error occurred within the High Availability subsystem, but the system has automatically recovered.
2. If the alarm occurs frequently, it is recommended to contact My Oracle Support.

31283 - Lost Communication with server

Alarm Group:
HA

Description:
Highly available server failed to receive mate heartbeats

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
comcolHaServerOfflineNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored; it clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues and/or it is recommended to contact My Oracle Support for assistance.

31284 - HA Remote Subscriber Heartbeat Warning

Alarm Group:
HA

Description:
High availability remote subscriber has not received a heartbeat within the configured interval.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRemoteHeartbeatWarningNotify

Recovery:

1. No action required. This is a warning and can be due to transient conditions. The remote subscriber will move to another server in the cluster.
2. If there continues to be no heartbeat from the server, it is recommended to contact My Oracle Support.

31285 - HA Node Join Recovery Entry

Alarm Group:
HA

Description:
High availability **node join** recovery entered

Severity:
Info

Instance:
Cluster set key of the DC outputting the event

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaSbrEntryNotify

Recovery:

1. No action required; this is a status message generated when one or more unaccounted for nodes join the designated coordinators group.

31286 - HA Node Join Recovery Plan

Alarm Group:
HA

Description:
High availability node join recovery plan

Severity:
Info

Instance:
Names of HA Policies (as defined in HA policy configuration)

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaSbrPlanNotify

Recovery:

1. No action required; this is a status message output when the designated coordinator generates a new action plan during node join recovery.

31287 - HA Node Join Recovery Complete

Alarm Group:
HA

Description:
High availability node join recovery complete

Severity:
Info

Instance:
Names of HA Policies (as defined in HA policy configuration)

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaSbrCompleteNotify

Recovery:

1. No action required; this is a status message output when the designated coordinator finishes running an action plan during node join recovery.

31288 - HA Site Configuration Error

Alarm Group
HA

Description
High availability site configuration error

Severity
Critical

Instance
GroupName, Policy ID, Site Name

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
comcolHaBadSiteCfgNotify

Recovery

1. If this alarm does not clear after correcting the configuration, it is recommended to contact My Oracle Support for assistance.

31290 - HA Process Status

Alarm Group:
HA

Description:
HA manager (cmha) status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaProcessStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31291 - HA Election Status

Alarm Group:
HA

Description:
HA DC Election status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaElectionStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31292 - HA Policy Status

Alarm Group:
HA

Description:
HA Policy plan status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaPolicyStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31293 - HA Resource Link Status

Alarm Group:
HA

Description:
This alarm is raised for nodes in our topology that we should be connected to (i.e., not OOS), but that we do not have any TCP links to it over any configured paths. It does not matter why the links were not established (networking connectivity, node not running, etc.).

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaLinkStatusNotify

Recovery:

1. If loss of communication between the active and standby servers is caused intentionally by maintenance activity, alarm can be ignored. It clears automatically when communication is restored between the two servers.
2. If communication fails at any other time, look for network connectivity issues.
3. If the problem persists, it is recommended to contact My Oracle Support.

31294 - HA Resource Status

Alarm Group:
HA

Description:
HA Resource registration status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaResourceStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31295 - HA Action Status

Alarm Group:
HA

Description:
HA Resource action status

Severity:
Info

Instance
N/A

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaActionStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31296 - HA Monitor Status

Alarm Group:
HA

Description:
HA Monitor action status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaMonitorStatusNotify

Recovery:

1. This event is used for internal logging. No action is required.

31297 - HA Resource Agent Info

Alarm Group:
HA

Description:
HA Resource Agent Info

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaInfoNotify

Recovery:

1. This event is used for internal logging. No action is required.

31298 - HA Resource Agent Detail

Alarm Group:
HA

Description:
Resource Agent application detailed information

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaRaDetailNotify

Recovery:

1. This event is used for internal logging. No action is required.

31299 - HA Notification Status

Alarm Group:
HA

Description:
HA Notification status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaNotificationNotify

Recovery:

1. No action required.

31300 - HA Control Status

Alarm Group:
HA

Description:
HA Control action status

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
300

OID:
comcolHaControlNotify

Recovery:

1. No action required.

31301 - HA Topology Events

Alarm Group:
HA

Description:
HA Topology events

Severity:
Info

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDsrHaTopologyNotify

Recovery:

1. No action required.

31322 - HA Configuration Error

Alarm Group
HA

Description
High availability configuration error

Severity
Minor

Instance
NodeID, or HA Tunnel ID

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
comcolHaBadCfgNotify

Recovery

1. It is recommended to contact 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

Recovery:

1. It is recommended to contact My Oracle Support to request hardware replacement.

32101 - Breaker Panel Breaker Failure

Alarm Group:
PLAT

Description:
Breaker Panel Breaker Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlBreakerFailure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32102 - Breaker Panel Monitoring Failure

Alarm Group:
PLAT

Description:
Breaker Panel Monitoring Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlMntFailure

Recovery

1. 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

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32104 - Power Supply 1 Failure

Alarm Group:
PLAT

Description:
Power Supply 1 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply1Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32105 - Power Supply 2 Failure

Alarm Group:
PLAT

Description:
Power Supply 2 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply2Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32106 - Power Supply 3 Failure

Alarm Group:
PLAT

Description:
Power Supply 3 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply3Failure

Recovery

1. 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:
tpdRaidFeedUnavailable

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32108 - Raid Power 1 Failure

Alarm Group:
PLAT

Description:
Raid Power 1 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidPower1Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32109 - Raid Power 2 Failure

Alarm Group:
PLAT

Description:
Raid Power 2 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidPower2Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32110 - Raid Power 3 Failure

Alarm Group:
PLAT

Description:
Raid Power 3 Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidPower3Failure

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32111 - Device Failure

Alarm Group:
PLAT

Description:
Device Failure

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceFailure

Recovery:

1. It is recommended to contact My Oracle Support to request hardware replacement.

32112 - Device Interface Failure

Alarm Group:
PLAT

Description:
Device Interface Failure. 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:
tpdDeviceIfFailure

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 has 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:
tpdEccUncorrectableError

Alarm ID:
TKSPLATCR14

Recovery:

1. 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:
tpdSNMPGetFailure

Alarm ID:
TKSPLATCR15

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 servers time was good.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDaemonNotSynchronizedFailure

Alarm ID:
TKSPLATCR16

Recovery:

1. Verify NTP settings and that NTP sources are providing accurate time.
   a. Ensure ntpd service is running with correct options: -x -g.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Type `/usr/sbin/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 the NTP date may resolve the issue.

> **Note:** Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. Reset ntpd:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

4. Conform to recommended NTP topology and strategy.
   - No fewer than tree references are recommended.
   - If selecting a different number, the number should be odd.
   - No intermediate reference should be a virtualized server.
   - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact My Oracle Support.

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:
tpdNTPTimeGoneBackwards

Alarm ID:
TKSPLATCR17

Recovery:

1. Verify NTP settings and NTP sources are providing accurate time.
   a. Ensure ntpd service is running with correct options: -x -g
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Type `/usr/sbin/ntpdc -c sysinfo` to check the current state of the ntpd daemon.
   d. Verify the ntp peer configuration; execute ntpq -p; and analyze the output. Verify peer data, such as tally code (first column before remote), remote, refid, stratum (st), and jitter, are valid for server.
   e. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server, then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, then restart the ntpd service.
3. If problem persists, then a reset the NTP date may resolve the issue.

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. Reset ntpd:
   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start
4. Conform to recommended NTP topology and strategy.
   - No fewer than tree references are recommended.
   - If selecting a different number, the number should be odd.
   - No intermediate reference should be a virtualized server.
   - Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document
5. If the problem persists, it is recommended to contact My Oracle Support.

32117 - TPD NTP Offset Check Failure

Alarm Group:
PLAT

Description:
This alarm indicates the NTP offset of the server that is currently being synced to is greater than the critical threshold.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpOffsetCheckFailure

Alarm ID:
TKSPLATCR18

Recovery:

1. Verify NTP settings and NTP sources can be reached.
   a. Ensure ntpd service is running using `ps -ef | grep` or `service ntpd status`.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Type `/usr/sbin/ntpdc -c sysinfo` to check the current state of the ntpd daemon.
   d. Verify the ntp peer configuration; execute ntpq -p; and analyze the output. Verify peer data, such as tally code (first column before remote), remote, refid, stratum (st), and jitter, are valid for server.
   e. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server, then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, then restart the ntpd service.
3. If problem persists, then a reset the NTP date may resolve the issue.

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

4. Conform to recommended NTP topology and strategy.
   - No fewer than tree references are recommended.

- If selecting a different number, the number should be odd.
- No intermediate reference should be a virtualized server.
- Additional recommendations and topology are available in NTP Strategy section in the DSR Hardware and Software Installation 1/2 customer document

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

32300 - Server fan failure

Alarm Group:
PLAT

Description:
This alarm indicates that a fan on the application server is either failing or has failed completely. In either case, there is a danger of component failure due to overheating.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFanError

Alarm ID:
TKSPLATMA1

Recovery:

1. Run Syscheck in Verbose mode to determine which server fan assemblies is failing and replace the fan assembly.
2. If the problem persists, it is recommended to contact My Oracle Support.

32301 - Server internal disk error

Alarm Group:
PLAT

Description:
This alarm indicates the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdIntDiskError

Alarm ID:
TKSPLATMA2

Recovery:

1. Run syscheck in verbose mode.
2. Determine the raid state of the mirrored disks, collect data:

   ```
   cat /proc/mdstat

   cat /etc/raidtab
   ```

3. It is recommended to contact My Oracle Support and provide the system health check output and collected data.

32302 - Server RAID disk error

Alarm Group:
PLAT

Description:
This alarm indicates that the offboard storage server had a problem with its hardware disks.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRaidDiskError

Alarm ID:
TKSPLATMA3

Recovery

1. 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:
tpdPlatformError

Alarm ID:
TKSPLATMA4

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:
tpdFileSystemError

Alarm ID:
TKSPLATMA5

Recovery:

1. Run syscheck in verbose mode.
2. Address full file systems identified in syscheck output, and run syscheck in verbose mode.
3. It is recommended to contact My Oracle Support and provide the system health check output.

32305 - Server Platform process error

Alarm Group:
PLAT

Description:
This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPlatProcessError

Alarm ID:
TKSPLATMA6

Recovery:

1. Rerun syscheck in verbose mode.
2. If the alarm has been cleared then the problem is solved..
3. If the alarm has not been cleared then determine the run level of the system.
4. If system run level is not 4 then determine why the system is operating at that run level.
5. If system run level is 4, determine why the required number of instances process(es) are not running.
6. If the alarm persists, it is recommended to contact My Oracle Support and provide the system health check output.

32306 - Server RAM shortage error

Alarm Group:
PLAT

Description:
Not Implemented.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRamShortageError

Recovery

1. It is recommended to contact My Oracle Support.

32307 - Server swap space shortage failure

Alarm Group:
PLAT

Description:
This alarm indicates that the server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwapSpaceShortageError

Alarm ID:
TKSPLATMA8

Recovery:

1. Run syscheck in verbose mode.
2. Determine processes using swap.

Note: One method to determine the amount of swap being used by process is:

```
grep VmSwap /proc/<process id>/status
```

---

3. It is recommended to contact My Oracle Support and provide the system health check output and process swap usage.

32308 - Server provisioning network error

Alarm Group:
PLAT

Description:
This alarm indicates that the connection between the server's ethernet interface and the customer network is not functioning properly.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdProvNetworkError

Alarm ID:
TKSPLATMA9

Recovery:

1. Verify that a customer-supplied cable labeled TO CUSTOMER NETWORK is securely connected to the appropriate server. Follow the cable to its connection point on the local network and verify this connection is also secure.
2. Test the customer-supplied cable labeled TO CUSTOMER NETWORK with an Ethernet Line Tester. If the cable does not test positive, replace it.
3. Have your network administrator verify that the network is functioning properly.
4. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the network administrator is unable to determine the exact origin of the problem, it is recommended to contact My Oracle Support.

32309 - Eagle Network A Error

Alarm Group:
PLAT

Description:
Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdEagleNetworkAError

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32310 - Eagle Network B Error

Alarm Group:
PLAT

Description:
Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdEagleNetworkBError

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32311 - Sync Network Error

Alarm Group:
PLAT

Description:
Uncorrectable ECC Memory Error -- This alarm indicates that chipset has detected an uncorrectable (multiple-bit) memory error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.

Severity:
Critical

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSyncNetworkError

Recovery

1. It is recommended to contact My Oracle Support to request hardware replacement.

32312 - Server disk space shortage error

Alarm Group:
PLAT

Description:
This alarm indicates that one of the following conditions has occurred:

- A file system has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the file system.
- More than 90% of the total number of available files have been allocated on the file system.
- A file system has a different number of blocks than it had when installed.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskSpaceShortageError

Alarm ID:
TKSPLATMA13

Recovery:

1. Run syscheck in verbose mode.
2. Examine contents of identified volume in syscheck output to determine if any large files are in the file system. Delete unnecessary files, or move files off of server. Capture output from "du -sx <file system>".
3. Capture output from "df -h" and "df -i" commands.
4. Determine processes using the file system(s) that have exceeded the threshold.

5. It is recommended to contact My Oracle Support and provide the system health check output and provide additional file system output.

32313 - Server default route network error

Alarm Group:
PLAT

Description:
This alarm indicates that the default network route of the server is experiencing a problem.

> **Caution:** When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDefaultRouteNetworkError

Recovery:

1. Run syscheck in verbose mode.
2. If the syscheck output is: `The default router at <IP_address> cannot be pinged`, the router may be down or unreachable. Do the following:
   a. Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
   b. Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
   c. Check with the router administrator to verify that the router is configured to reply to pings on that interface.
   d. Rerun syscheck.
   e. If the alarm has not been cleared, it is recommended to collect the syscheck output and contact My Oracle Support.

3. If the syscheck output is: `The default route is not on the provisioning network`, it is recommended to collect the syscheck output and contact My Oracle Support.
4. If the syscheck output is: `An active route cannot be found for a configured default route`, it is recommended to collect the syscheck output and contact My Oracle Support.

32314 - Server temperature error

Alarm Group:
PLAT

Description:
The internal temperature within the server is unacceptably high.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerTemperatureError

Alarm ID:
TKSPLATMA15

Recovery:

1. Ensure that nothing is blocking the fan intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Run syscheck.
   a. If the alarm has been cleared, the problem is resolved.
   b. If the alarm has not been cleared, continue troubleshooting.
4. Replace the filter.

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

5. Re-run syscheck.
   a. If the alarm has been cleared, the problem is resolved.
   b. If the alarm has not been cleared, continue troubleshooting.
6. If the problem has not been resolved, it is recommended to contact My Oracle Support.

32315 - Server mainboard voltage error

Alarm Group:
PLAT

Description:
This alarm indicates that one or more of the monitored voltages on the server 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

Recovery:

1. Run syscheck in verbose mode.
2. If the alarm persists, it is recommended to contact My Oracle Support and provide the system health check output.

32316 - Server power feed error

Alarm Group:
PLAT

Description:
This alarm indicates that one of the power feeds to the server has failed. If this alarm occurs in conjunction with any Breaker Panel alarm, there might be a problem with the breaker panel.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerFeedError

Alarm ID:
TKSPLATMA17

Recovery:

1. Verify that all the server power feed cables to the server that is reporting the error are securely connected.
2. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
3. Follow the power feed to its connection on the power source. Ensure that the power source is ON and that the power feed is properly secured.
4. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
5. If the power source is functioning properly and the wires are all secure, have an electrician check the voltage on the power feed.
6. Check to see if the alarm has cleared
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, continue with the next step.
7. If the problem has not been resolved, it is recommended to contact My Oracle Support.

32317 - Server disk health test error

Alarm Group:
PLAT

Description:
Either the hard drive has failed or failure is imminent.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskHealthError

Alarm ID:
TKSPLATMA18

Recovery:

1. Run syscheck in verbose mode.
2. Replace the hard drives that have failed or are failing.
3. Re-run syscheck in verbose mode.
4. Perform the recovery procedures for the other alarms that may accompany this alarm.
5. If the problem has not been resolved, it is recommended to contact My Oracle Support and provide the system health check output. .

32318 - Server disk unavailable error

Alarm Group:
PLAT

Description:
The `smartd` service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskUnavailableError

Alarm ID:
TKSPLATMA19

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support and provide the system health check output.

32319 - Device error

Alarm Group:
PLAT

Description:
This alarm indicates that the offboard storage server had a problem with its disk volume filling up.

Severity:
Major

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceError

Alarm ID:
TKSPLATMA20

Recovery

1. It is recommended to contact the My Oracle Support.

32320 - Device interface error

Alarm Group:
PLAT

Description:
This alarm indicates that the IP bond is either not configured or down.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceIfError

Alarm ID:
TKSPLATMA21

Recovery:

1. Run syscheck in verbose mode.
2. Investigate the failed bond, and slave devices, configuration:
   a. Navigate to /etc/sysconfig/network-scripts for the persistent configuration of a device.
3. Determine if the failed bond, and slave devices, has been administratively shut down or has operational issues:
   a. cat /proc/net/bonding/bondX, where X is bond designation
   b. ethtool <slave device>
4. If bond, and slaves, are healthy attempt to administratively bring bond up:
   a. ifup bondX
5. If the problem has not been resolved, it is recommended to contact My Oracle Support and provide the system health check output and the output of the above investigation.

32321 - Correctable ECC memory error

Alarm Group:
PLAT

Description:
This alarm indicates that chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdEccCorrectableError

Alarm ID:
TKSPLATMA22

Recovery:

1. No recovery necessary.
2. If the condition persists, verify the server firmware. Update the firmware if necessary, and re-run syscheck in verbose mode. Otherwise if the condition persists and the firmware is up to date, contact the hardware vendor to request hardware replacement.

32322 - Power Supply A error

Alarm Group:
PLAT

Description:
This alarm indicates that power supply 1 (feed A) has failed.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply1Error

Alarm ID:
TKSPLATMA23

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.

2. Run syscheck in verbose mode. The output will provide details about what is wrong with the power supply.
3. If the problem persists, it is recommended to contact My Oracle Support and provide the syscheck verbose output. Power supply 1 (feed A) will probably need to be replaced.

32323 - Power Supply B error

Alarm Group:
PLAT

Description:
This alarm indicates that power supply 2 (feed B) has failed.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdPowerSupply2Error

Alarm ID:
TKSPLATMA24

Recovery:

1. Verify that nothing is obstructing the airflow to the fans of the power supply.
2. Run syscheck in verbose mode. The output will provide details about what is wrong with the power supply.
3. If the problem persists, it is recommended to contact My Oracle Support and provide the syscheck verbose output. Power supply 2 (feed B) will probably need to be replaced.

32324 - Breaker panel feed error

Alarm Group:
PLAT

Description:
This alarm indicates that the server is not receiving information from the breaker panel relays.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlFeedError

Alarm ID:
TKSPLATMA25

Recovery:

1. Verify that the same alarm is displayed by multiple servers:
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by multiple servers, go to the next step.
2. Verify that the cables that connect the servers to the breaker panel are not damaged and are securely fastened to both the Alarm Interface ports on the breaker panel and to the serial ports on both servers.
3. If the problem has not been resolved, it is recommended to contact My Oracle Support to request that the breaker panel be replaced.

32325 - Breaker panel breaker error

Alarm Group:
PLAT

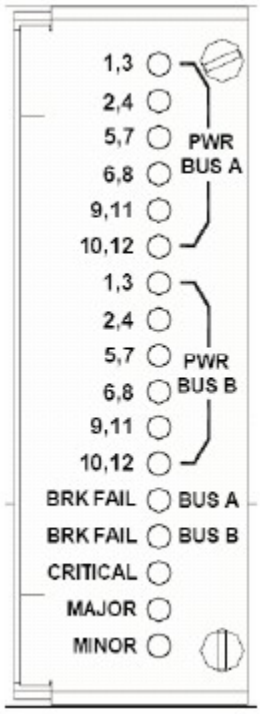
Description:
This alarm indicates that a power fault has been identified by the breaker panel. The LEDs on the center of the breaker panel (see Figure 4-1) identify whether the fault occurred on the input power or the output power, as follows:

- A power fault on input power (power from site source to the breaker panel) is indicated by one of the LEDs in the PWR BUS A or PWR BUS B group illuminated Red. In general, a fault in the input power means that power has been lost to the input power circuit.

> **Note:** LEDs in the PWR BUS A or PWR BUS B group that correspond to unused feeds are not illuminated; LEDs in these groups that are not illuminated do not indicate problems.

- A power fault on output power (power from the breaker panel to other frame equipment) is indicated by either BRK FAIL BUS A or BRK FAIL BUS B illuminated RED. This type of fault can be caused by a surge or some sort of power degradation or spike that causes one of the circuit breakers to trip.

Figure 4-1 Breaker Panel LEDs



Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
TPDBrkPnlBreakerError

Alarm ID:
TKSPLATMA26

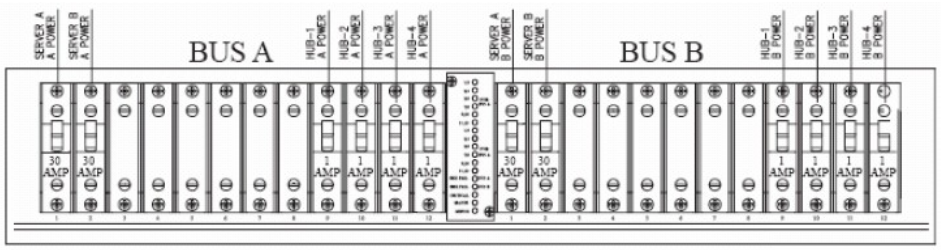
Recovery:

1. Verify that the same alarm is displayed by both servers. The single breaker panel normally sends alarm information to both servers:

- If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
- If this alarm is displayed by both servers, go to the next step.

2. For each breaker assignment, verify that the corresponding LED in the PWR BUS A group and the PWR BUS B group is illuminated Green.

Figure 4-2 Breaker Panel Setting



If one of the LEDs in the PWR BUS A group or the PWR BUS B group is illuminated Red, a problem has been detected with the corresponding input power feed. Perform the following steps to correct this problem:

- Verify that the customer provided source for the affected power feed is operational. If the power source is properly functioning, have an electrician remove the plastic cover from the rear of the breaker panel and verify the power source is indeed connected to the input power feed connector on the rear of the breaker panel. Correct any issues found.
- Check the LEDs in the PWR BUS A group and the PWR BUS B group again.
  - **a.** If the LEDs are now illuminated Green, the issue has been resolved. Proceed to step 4 to verify that the alarm has been cleared.
  - **b.** If the LEDs are still illuminated Red, continue to the next sub-step.
- Have the electrician verify the integrity of the input power feed. The input voltage should measure nominally -48VDC (that is, between -41VDC and -60VDC). If the supplied voltage is not within the acceptable range, the input power source must be repaired or replaced.

Note:

Be sure the voltmeter is connected properly. The locations of the BAT and RTN connections are in mirror image on either side of the breaker panel.

If the measured voltage is within the acceptable range, the breaker panel may be malfunctioning. The breaker panel must be replaced.

- Check the LEDs in the PWR BUS A group and the PWR BUS B group again after the necessary actions have been taken to correct any issues found.
  - **a.** If the LEDs are now illuminated Green, the issue has been resolved and proceed to step 4 to verify that the alarm has been cleared.
  - **b.** If the LEDs are still illuminated Red, skip to step 5

3. Check the BRK FAIL LEDs for BUS A and for BUS B.

   - If one of the BRK FAIL LEDs is illuminated Red, then one or more of the respective Input Breakers has tripped. (A tripped breaker is indicated by the toggle located in the center position.) Perform the following steps to repair this issue:

   a. For all tripped breakers, move the breaker down to the open (OFF) position and then back up to the closed (ON) position.

   b. After all the tripped breakers have been reset, check the BRK FAIL LEDs again. If one of the BRK FAIL LEDs is still illuminated Red, run syscheck and contact My Oracle Support.

4. If all of the BRK FAIL LEDs and all the LEDs in the PWR BUS A group and the PWR BUS B group are illuminated Green, there is most likely a problem with the serial connection between the server and the breaker panel. This connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables are properly secured. If any issues are discovered with these cable connections, make the necessary corrections and continue to the next step to verify that the alarm has been cleared, otherwise it is recommended to run syscheck and contact My Oracle Support.

5. Run syscheck.

   - If the alarm has been cleared, the problem is resolved.
   - If the problem has not been resolved, it is recommended to contact My Oracle Support.

32326 - Breaker panel monitoring error

Alarm Group:
PLAT

Description:
This alarm indicates a failure in the hardware and/or software that monitors the breaker panel. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself.

Note: When this alarm occurs, the system is unable to monitor the breaker panel for faults. Thus, if this alarm is detected, it is imperative that the breaker panel be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm:

- 32324 – Breaker panel feed error
- 32325 – Breaker panel breaker error

until the Breaker Panel Monitoring Error has been corrected.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdBrkPnlMntError

Alarm ID:
TKSPLATMA27

Recovery:

1. Verify that the same alarm is displayed by both servers (the single breaker panel normally sends alarm information to both servers):
   - If this alarm is displayed by only one server, the problem is most likely to be with the cable or the server itself. Look for other alarms that indicate a problem with the server and perform the recovery procedures for those alarms first.
   - If this alarm is displayed by both servers, go to the next step.
2. Verify that both ends of the labeled serial cables are secured properly (for locations of serial cables, see the appropriate hardware manual).
3. Run syscheck..
   - If the alarm has been cleared, the problem is resolved.
   - If the alarm has not been cleared, it is recommended to contact My Oracle Support.

32327 - Server HA Keepalive error

Alarm Group:
PLAT

Description:
This alarm indicates that heartbeat process has detected that it has failed to receive a heartbeat packet within the timeout period.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaKeepaliveError

Alarm ID:
TKSPLATMA28

Recovery:

1. Determine if the mate server is currently down and bring it up if possible.
2. Determine if the keepalive interface is down.
3. Determine if 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 that **DRBD** is not functioning properly on the local server. The DRBD state (disk state, node state, and/or connection state) indicates a problem.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDrbdUnavailable

Alarm ID:
TKSPLATMA29

Recovery

1. It is recommended to contact My Oracle Support.

32329 - DRBD is not replicating

Alarm Group:
PLAT

Description:
This alarm indicates that DRBD is not replicating to the peer server. Usually this indicates that DRBD is not connected to the peer server. It is possible that a DRBD Split Brain has occurred.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDrbdNotReplicating

Alarm ID:
TKSPLATMA30

Recovery

1. It is recommended to contact My Oracle Support.

32330 - DRBD peer problem

Alarm Group:
PLAT

Description:
This alarm indicates that DRBD is not functioning properly on the peer server. DRBD is connected to the peer server, but the DRBD state on the peer server is either unknown or indicates a problem.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDrbdPeerProblem

Alarm ID:
TKSPLATMA31

Recovery

1. It is recommended to contact the My Oracle Support.

32331 - HP disk problem

Alarm Group:
PLAT

Description:
This major alarm indicates that there is an issue with either a physical or logical disk in the **HP** disk subsystem. The message will include the drive type, location, slot and status of the drive that has the error.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskProblem

Alarm ID:
TKSPLATMA32

Recovery:

1. Run syscheck in verbose mode.
2. If "Cache Status" is OK and "Cache Status Details" reports a cache error was detected so diagnostics should be run, there probably is no battery and data was left over in the write cache not getting flushed to disk and won't since there is no battery.
3. If "Cache Status" is "Permanently Disabled" and "Cache Status Details" indicated the cache is disabled, if there is no battery then the firmware should be upgraded.
4. Re-run syscheck in verbose mode if firmware upgrade was necessary.

5. If the condition persists, it is recommended to contact My Oracle Support and provide the system health check output. The disk may need to be replaced.

32332 - HP Smart Array controller problem

Alarm Group:
PLAT

Description:
This major alarm indicates that there is an issue with an HP disk controller. The message will include the slot location, the component on the controller that has failed, and status of the controller that has the error.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskCtrlrProblem

Alarm ID:
TKSPLATMA33

Recovery:

1. Run syscheck in verbose mode.
2. If condition persists, it is recommended to contact My Oracle Support and provide the system health check output.

32333 - HP hpacucliStatus utility problem

Alarm Group:
PLAT

Description:
This major alarm indicates that there is an issue with the process that caches the HP disk subsystem status. This usually means that the hpacucliStatus/hpDiskStatus daemon is either not running, or hung.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHPACUCLIProblem

Alarm ID:
TKSPLATMA34

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. Determine if the HP disk status daemon is running. If not running verify that it was not administratively stopped.

   Note: The disk status daemon is named either TKLChpacucli or TPDhpDiskStatus in more recent versions of TPD.

   a. Executing "status TPDhpDiskStatus", or "status TKLChpacucli" depending on TPD release, should produce output indicating that the process is running.
4. If not running, attempt to start the HP disk status process :

   "start TPDhpDiskStatus", or if appropriate "start TKLChpacucli" .
5. Verify that there are no hpssacli, or hpacucli, error messages in /var/log/messages. If there are this could indicate that the HP utility is hung. If the HP hpssacli utility, or hpacucli utility, is hung, proceed with next step.
6. It is recommended to contact My Oracle Support and provide the system health check output, and savelogs_plat output.

32334 - Multipath device access link problem

Alarm Group:
PLAT

Description:
One or more "access paths" of a multipath device are failing or are not healthy, or the multipath device does not exist.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMpathDeviceProblem

Recovery:

1. It is recommended to contact My Oracle Support.

32335 - Switch link down error

Alarm Group:
PLAT

Description:
The link is down.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwitchLinkDownError

Alarm ID:
TKSPLATMA36

Recovery:

1. Verify the cabling between the port and the remote side.
2. Verify networking on the remote end.
3. If the problem persists, it is recommended to contact My Oracle Support to determine who should verify port settings on both the server and the switch.

32336 - Half Open Socket Limit

Alarm Group:
PLAT

Description:
This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHalfOpenSockLimit

Alarm ID:
TKSPLATMA37

Recovery:

1. Run syscheck in verbose mode.
2. Determine what process and address reports a state of SYN_RECV and collect data:
   - netstat -nap.
3. It is recommended to contact My Oracle Support and provide the system health check output and collected data.

32337 - Flash Program Failure

Alarm Group:
PLAT

Description:
This alarm indicates that there was an error while trying to update the firmware flash on the E5-APP-B cards.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFlashProgramFailure

Alarm ID:
TKSPLATMA38

Recovery:

1. It is recommended to contact My Oracle Support.

32338 - Serial Mezzanine Unseated

Alarm Group:
PLAT

Description:
This alarm indicates that a connection to the serial mezzanine board may not be properly seated.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSerialMezzUnseated

Alarm ID:
TKSPLATMA39

Recovery:

1. Ensure that both ends of both cables connecting the serial mezzanine card to the main board are properly seated into their connectors.
2. It is recommended to contact My Oracle Support if reseating the cables does not clear the alarm.

32339 - TPD Max Number Of Running Processes Error

Alarm Group:
PLAT

Description:
This alarm indicates that the maximum number of running processes has reached the major threshold.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMaxPidLimit

Alarm ID:
TKSPLATMA40

Recovery:

1. Run syscheck in verbose mode.
2. Execute 'pstree' to see what pids are on the system and what process created them. Collect the output of command, and review the output to determine the process responsible for the alarm.
3. It is recommended to contact My Oracle Support and provide the system health check output, and pid output.

32340 - TPD NTP Daemon Not Synchronized Error

Alarm Group:
PLAT

Description:
This alarm indicates that the server is not synchronized to an NTP source and has not been synchronized for an extended number of hours and has reached the major threshold.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDaemonNotSynchronizedError

Alarm ID:
TKSPLATMA41

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

   Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

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

32341 - TPD NTP Daemon Not Synchronized Error

Alarm Group:
PLAT

Description:
This alarm indicates that the server is not synchronized to an NTP source and has never been synchronized since the last configuration change.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDaemonNeverSynchronized

Alarm ID:
TKSPLATMA42

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If the ntp peer is reachable, restart the ntpd service.
3. If the problem persists then a reset the NTP date may resolve the issue.

   Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

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

32342 - NTP Offset Check Error

Alarm Group:
PLAT

Description:
This alarm indicates the NTP offset of the server that is currently being synced to is greater than the major threshold.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpOffsetCheckError

Alarm ID:
TKSPLATMA43

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If the ntp peer is reachable, restart the ntpd service.
3. If the problem persists then a reset the NTP date may resolve the issue.

   Note: Prior to the reset of the ntp date the applications may need to be stopped, and subsequent to the ntp reset, the application restarted.

   a. To reset date:
   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start
4. If the problem persists, it is recommended to contact My Oracle Support.

32343 - TPD RAID disk

Alarm Group:
PLAT

Description:
This alarms indicates that physical disk or logical volume on RAID controller is not in optimal state as reported by syscheck.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskProblem

Alarm ID:
TKSPLATMA44

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support and provide the system health check output.

32344 - TPD RAID controller problem

Alarm Group:
PLAT

Description:
This alarms indicates that RAID controller needs intervention.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskCtrlrProblem

Alarm ID:
TKSPLATMA45

Recovery:

1. Run syscheck in verbose mode.
2. Verify firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.
3. It is recommended to contact My Oracle Support and provide the system health check output.

32345 - Server Upgrade snapshot(s) invalid

Alarm Group:
PLAT

Description:
This alarm indicates that upgrade snapshot(s) are invalid and backout is no longer possible.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdUpgradeSnapshotInvalid

Alarm ID:
TKSPLATMA46

Recovery:

1. Run accept to remove invalid snapshot(s) and clear alarms.
2. If the alarm persists, it is recommended to contact My Oracle Support.

32346 - OEM hardware management service reports an error

Alarm Group:
PLAT

Description:
This alarms indicates that OEM hardware management service reports an error.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdOEMHardware

Alarm ID:
TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support and provide the system health check output.

32347 - The hwmgmtcliStatus daemon needs intervention

Alarm Group:
PLAT

Description:
This alarms indicates the hwmgmtcliStatus daemon is not running or is not responding.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHWMGMTCLIProblem

Alarm ID:
TKSPLATMA47

Recovery:

1. Run syscheck in verbose mode.
2. Verify the firmware is up to date for the server, if not up to date upgrade firmware, and re-run syscheck in verbose mode.

3. Determine if the hwmgmtd process is running. If not running verify that it was not administratively stopped.
   - Executing "service hwmgmtd status" should produce output indicating that 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 that it was not administratively stopped.
   - Executing "status TKLChwmgmtcli" should produce output indicating that the process is running.
   - If not running attempt to start process "start TKLChwmgmtcli".
5. Verify that there are no hwmgmt error messages in /var/log/messages. If there are this could indicate that the Oracle utility is hung. If 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:
tpdFipsSubsystemProblem

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support and provide the system health check output.

32349 - File Tampering

Alarm Group:
PLAT

Description:
This alarm indicates **HIDS** has detected file tampering.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHidsFileTampering

Recovery:

1. It is recommended to contact My Oracle Support.

32350 - Security Process Terminated

Alarm Group:
PLAT

Description:
This alarm indicates that the security process monitor is not running.

Severity:
Major

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSecurityProcessDown

Recovery:

1. It is recommended to contact My Oracle Support.

32500 - Server disk space shortage warning

Alarm Group:
PLAT

Description:
This alarm indicates that one of the following conditions has occurred:

- A file system has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the file system.
- More than 80% (but less than 90%) of the total number of available files have been allocated on the file system.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskSpaceShortageWarning

Alarm ID:
TKSPLATMI1

Recovery:

1. Run syscheck in verbose mode.
2. Examine contents of identified volume in syscheck output to determine if any large files are in the file system. Delete unnecessary files, or move files off of server. Capture output from "du -sx <file system>".
3. Capture output from "df -h" and "df -i" commands.
4. Determine processes using the file system(s) that have exceeded the threshold.
5. It is recommended to contact My Oracle Support, provide the system health check output, and provide additional file system output.

32501 - Server application process error

Alarm Group:
PLAT

Description:
This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdApplicationProcessError

Alarm ID:
TKSPLATMI2

Recovery:

1. Run syscheck in verbose mode.
2. If the alarm has been cleared, then the problem is solved.
3. If the alarm has not been cleared, determine the run level of the system.
   - If system run level is not 4, determine why the system is operating at that run level.
   - If system run level is 4, determine why the required number of instances processes are not running.
4. For additional assistance, it is recommended to contact My Oracle Support and provide the syscheck output.

32502 - Server hardware configuration error

Alarm Group:
PLAT

Description:
This alarm indicates that one or more of the server's hardware components are not in compliance with specifications (refer to the appropriate hardware manual).

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHardwareConfigError

Alarm ID:
TKSPLATMI3

Recovery:

1. Run syscheck in verbose mode.
2. Contact the hardware vendor to request a hardware replacement.

32503 - Server RAM shortage warning

Alarm Group:
PLAT

Description:
This alarm is generated by the **MPS** syscheck software package and is not part of the TPD distribution.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdRamShortageWarning

Alarm ID:
TKSPLATMI4

Recovery

1. Refer to MPS-specific documentation for information regarding this alarm.
2. It is recommended to contact My Oracle Support.

32504 - Software Configuration Error

Alarm Group:
PLAT

Description:
This alarm is generated by the MPS syscheck software package and is not part of the PLAT distribution.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSoftwareConfigError

Recovery

1. It is recommended to contact My Oracle Support.

32505 - Server swap space shortage warning

Alarm Group:
PLAT

Description:
This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

> **Note:** For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSwapSpaceShortageWarning

Alarm ID:
TKSPLATMI6

Recovery:

1. Run syscheck in verbose mode.
2. Determine which processes are using swap.
   a. List application processes and determine the process id.
   b. 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 that 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 that the modifications will not impact the method of connectivity for the current login session. It is also crucial that 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

Recovery:

1. Run syscheck in verbose mode.
2. If the syscheck output is: `The default router at <IP_address> cannot be pinged`, the router may be down or unreachable. Do the following:
   a. Verify the network cables are firmly attached to the server and the network switch, router, hub, etc.
   b. Verify that the configured router is functioning properly. Check with the network administrator to verify the router is powered on and routing traffic as required.
   c. Check with the router administrator to verify that the router is configured to reply to pings on that interface.
   d. Rerun syscheck.
3. If the alarm has not cleared, it is recommended to collect the syscheck output and contact My Oracle Support.

32507 - Server temperature warning

Alarm Group:
PLAT

Description:
This alarm indicates that the internal temperature within the server is outside of the normal operating range. A server Fan Failure may also exist along with the Server Temperature Warning.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerTemperatureWarning

Alarm ID:
TKSPLATMI8

Recovery:

1. Ensure that nothing is blocking the fan intake. Remove any blockage.
2. Verify that the temperature in the room is normal. If it is too hot, lower the temperature in the room to an acceptable level.

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the room returns to an acceptable temperature before the alarm cleared.

3. Run syscheck.
4. Replace the filter (refer to the appropriate hardware manual).

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. It may take about ten minutes after the filter is replaced before the alarm cleared.

5. Run syscheck.
6. If the problem has not been resolved, it is recommended to contact My Oracle Support.

32508 - Server core file detected

Alarm Group:
PLAT

Description:
This alarm indicates that an application process has failed and debug information is available.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerCoreFileDetected

Alarm ID:
TKSPLATMI9

Recovery:

1. It is recommended to contact My Oracle Support to create a service request.
2. On the affected server, 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 that the **NTP daemon** (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPDeamonNotSynchronizedWarning

Alarm ID:
TKSPLATMI10

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.

2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

> **Note:** Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

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

32510 - CMOS battery voltage low

Alarm Group:
PLAT

Description:
The presence of this alarm indicates that the **CMOS** battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdCMOSBatteryVoltageLow

Alarm ID:
TKSPLATMI11

Recovery:

1. It is recommended to contact My Oracle Support.

32511 - Server disk self test warning

Alarm Group:
PLAT

Description:
A non-fatal disk issue (such as a sector cannot be read) exists.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdSmartTestWarn

Alarm ID:
TKSPLATMI12

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support.

32512 - Device warning

Alarm Group:
PLAT

Description:
This alarm indicates that either we are unable to perform an `snmpget` command on the configured SNMP OID or the value returned failed the specified comparison operation.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceWarn

Alarm ID:
TKSPLATMI13

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support.

32513 - Device interface warning

Alarm Group:
PLAT

Description:
This alarm can be generated by either an SNMP trap or an IP bond error.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDeviceIfWarn

Alarm ID:
TKSPLATMI14

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support.

32514 - Server reboot watchdog initiated

Alarm Group:
PLAT

Description:
This alarm indicates that the hardware watchdog was not strobed by the software and so the server rebooted the server. This applies to only the last reboot and is only supported on a T1100 application server.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdWatchdogReboot

Alarm ID:
TKSPLATMI15

Recovery:

1. It is recommended to contact My Oracle Support.

32515 - Server HA failover inhibited

Alarm Group:
PLAT

Description:
This alarm indicates that the server has been inhibited and therefore HA failover is prevented from occurring.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaInhibited

Alarm ID:
TKSPLATMI16

Recovery:

1. It is recommended to contact My Oracle Support.

32516 - Server HA Active to Standby transition

Alarm Group:
PLAT

Description:
This alarm indicates that the server is in the process of transitioning HA state from Active to Standby.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaActiveToStandbyTrans

Alarm ID:
TKSPLATMI17

Recovery:

1. It is recommended to contact My Oracle Support.

32517 - Server HA Standby to Active transition

Alarm Group:
PLAT

Description:
This alarm indicates that the server is in the process of transitioning HA state from Standby to Active.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHaStandbyToActiveTrans

Alarm ID:
TKSPLATMI18

Recovery:

1. It is recommended to contact My Oracle Support.

32518 - Platform Health Check failure

Alarm Group:
PLAT

Description:
This alarm is used to indicate a configuration error.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHealthCheckFailed

Alarm ID:
TKSPLATMI19

Recovery:

1. It is recommended to contact My Oracle Support.

32519 - NTP Offset Check failure

Alarm Group:
PLAT

Description:
This minor alarm indicates that time on the server is outside the acceptable range (or offset) from the NTP server. The Alarm message will provide the offset value of the server from the **NTP** server and the offset limit that the application has set for the system.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpOffsetCheckWarning

Alarm ID:
TKSPLATMI20

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start

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

32520 - NTP Stratum Check failure

Alarm Group:
PLAT

Description:
This alarm indicates that NTP is syncing to a server, but the stratum level of the NTP server is outside of the acceptable limit. The Alarm message will provide the stratum value of the NTP server and the stratum limit that the application has set for the system.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
ntpStratumCheckFailed

Alarm ID:
TKSPLATMI21

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:
   - sudo service ntpd stop
   - sudo ntpdate <ntp server ip>
   - sudo service ntpd start
4. If the problem persists, it is recommended to contact My Oracle Support.

32521 - SAS Presence Sensor Missing

Alarm Group:
PLAT

Description:
This alarm indicates that the T1200 server drive sensor is not working.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sasPresenceSensorMissing

Alarm ID:
TKSPLATMI22

Recovery:

1. It is recommended to contact My Oracle Support to get a replacement sensor.

32522 - SAS Drive Missing

Alarm Group:
PLAT

Description:
This alarm indicates that the number of drives configured for this server is not being detected.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
sasDriveMissing

Alarm ID:
TKSPLATMI23

1. It is recommended to contact My Oracle Support.

32523 - DRBD failover busy

Alarm Group:
PLAT

Description:
This alarm indicates that a DRBD sync is in progress from the peer server to the local server. The local server is not ready to act as the primary DRBD node, since it's data is not up to date.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDrbdFailoverBusy

Alarm ID:
TKSPLATMI24

Recovery

1. A DRBD sync should not take more than 15 minutes to complete. Please wait for approximately 20 minutes, and then check if the DRBD sync has completed. If the alarm persists longer than this time period, it is recommended to contact My Oracle Support.

32524 - HP disk resync

Alarm Group:
PLAT

Description:
This minor alarm indicates that the HP disk subsystem is currently resynchronizing after a failed or replaced drive, or some other change in the configuration of the HP disk subsystem. The output of the message will include the disk that is resynchronizing and the percentage complete. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHpDiskResync

Alarm ID:
TKSPLATMI25

Recovery:

1. Run syscheck in verbose mode.
2. If the percent recovering is not updating, wait at least 5 minutes between subsequent runs of syscheck.
3. If the alarm persists, it is recommended to contact My Oracle Support and provide the syscheck output.

32525 - Telco Fan Warning

Alarm Group:
PLAT

Description:
This alarm indicates that the Telco switch has detected an issue with an internal fan.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdTelcoFanWarning

Alarm ID:
TKSPLATMI26

Recovery:

1. Contact the vendor to get a replacement switch. Verify the ambient air temperature around the switch is as low as possible until the switch is replaced.

Note: My Oracle Support personnel can perform an `snmpget` command or log into the switch to get detailed fan status information.

32526 - Telco Temperature Warning

Alarm Group:
PLAT

Description:
This alarm indicates that the Telco switch has detected the internal temperature has exceeded the threshold.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdTelcoTemperatureWarning

Alarm ID:
TKSPLATMI27

Recovery:

1. Lower the ambient air temperature around the switch as low as possible.
2. If the problem persists, it is recommended to contact My Oracle Support.

32527 - Telco Power Supply Warning

Alarm Group:
PLAT

Description:
This alarm indicates that the Telco switch has detected that one of the duplicate power supplies has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdTelcoPowerSupplyWarning

Alarm ID:
TKSPLATMI28

Recovery:

1. Verify the breaker was not tripped.
2. If the breaker is still good and problem persists, it is recommended to contact My Oracle Support who can perform a `snmpget` command or log into the switch to determine which power supply is failing. If the power supply is bad, the switch must be replaced.

32528 - Invalid BIOS value

Alarm Group:
PLAT

Description:
This alarm indicates that the HP server has detected that one of the setting for either the embedded serial port or the virtual serial port is incorrect.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdInvalidBiosValue

Alarm ID:
TKSPLATMI29

Recovery:

1. Change the BIOS values to the expected values which involves re-booting the server. It is recommended to contact My Oracle Support for directions on changing the **BIOS**.

32529 - Server Kernel Dump File Detected

Alarm Group:
PLAT

Description:
This alarm indicates that the kernel has crashed and debug information is available.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerKernelDumpFileDetected

Alarm ID:
TKSPLATMI30

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support.

32530 - TPD Upgrade Failed

Alarm Group:
PLAT

Description:
This alarm indicates that a TPD upgrade has failed.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
TpdServerUpgradeFailed

Alarm ID:
TKSPLATMI31

Recovery:

1. It is recommended to contact My Oracle Support.

32531 - Half Open Socket Warning Limit

Alarm Group:
PLAT

Description
This alarm indicates that the number of half open TCP sockets has reached the major threshold. This problem is caused by a remote system failing to complete the TCP 3-way handshake.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdHalfOpenSocketWarning

Alarm ID:
TKSPLATMI32

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support.

32532 - Server Upgrade Pending Accept/Reject

Alarm Group:
PLAT

Description:
This alarm indicates an upgrade occurred but has not been accepted or rejected yet.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdServerUpgradePendingAccept

Alarm ID:
TKSPLATMI33

Recovery:

1. Follow the steps in the application procedure to accept or reject the upgrade.

32533 - TPD Max Number Of Running Processes Warning

Alarm Group:
PLAT

Description:
This alarm indicates that the maximum number of running processes has reached the minor threshold.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdMaxPidWarning

Alarm ID:
TKSPLATMI34

Recovery:

1. Run syscheck in verbose mode.
2. It is recommended to contact My Oracle Support.

32534 - TPD NTP Source Is Bad Warning

Alarm Group:
PLAT

Description:
This alarm indicates that an NTP source has been rejected by the NTP daemon and is not being considered as a time source.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdNTPSourceIsBad

Alarm ID:
TKSPLATMI35

Recovery:

1. Verify NTP settings and that NTP sources can be reached.
   a. Ensure ntpd service is running.
   b. Verify the content of the /etc/ntp.conf file is correct for the server.
   c. Verify the ntp peer configuration; execute ntpq -p and analyze the output. Verify peer data, (such as tally code (first column before "remote"), remote, refid, stratum (st), and jitter), are valid for server.
   d. Execute ntpstat to determine the ntp time synchronization status. If not synchronized or the stratum is not correct for server then ping the ntp peer to determine if peer can be reached.
2. If ntp peer is reachable, restart the ntpd service.
3. If problem persists then a reset the NTP date may resolve the issue.

   Note: Before resetting the ntp date, the applications may need to be stopped; and subsequent to the ntp reset, the application restarted.

   a. To reset date:

   - sudo service ntpd stop

- sudo ntpdate <ntp server ip>
- sudo service ntpd start

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

32535 - TPD RAID disk resync

Alarm Group:
PLAT

Description:
This alarm indicates that the RAID logical volume is currently resyncing after a failed/replaced drive, or some other change in the configuration. The output of the message will include the disk that is resyncing. This alarm should eventually clear once the resync of the disk is completed. The time it takes for this is dependent on the size of the disk and the amount of activity on the system (rebuild of 600G disks without any load takes about 75min).

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdDiskResync

Alarm ID:
TKSPLATMI36

Recovery:

1. Run syscheck in verbose mode.
2. If this alarm persists for several hours (depending on a load of a server, rebuilding an array can take multiple hours to finish), it is recommended to contact My Oracle Support.

32536 - TPD Server Upgrade snapshot(s) warning

Alarm Group:
PLAT

Description:
This alarm indicates that upgrade snapshot(s) are above configured threshold and either accept or reject of LVM upgrade has to be run soon, otherwise snapshots will become full and invalid.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdUpgradeSnapshotWarning

Alarm ID:
TKSPLATMI37

Recovery:

1. Run accept or reject of current LVM upgrade before snapshots become invalid.
2. It is recommended to contact My Oracle Support.

32537 - FIPS subsystem warning event

Alarm Type:
PLAT

Description:
This alarm indicates that the FIPS subsystem requires a reboot in order to complete configuration.

Severity:
Minor

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

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdFipsSubsystemWarning

Recovery

1. If alarm doesn't clear on its own, it is recommended to contact My Oracle Support.

32538 - Platform Data Collection Error

Alarm Group
PLAT

Description
Platform Data Collection Error.

Severity
Minor

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

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
tpdPdcError

Recovery

1. Run `/usr/TKLC/plat/bin/pdcAdm`. If ran as admusr, use sudo to run the command.
2. If this command fails, it is recommended to collect the output and contact My Oracle Support.

32539 - Server Patch Pending Accept/Reject

Alarm Group
PLAT

Description
Server Patch Pending Accept/Reject.

Severity
Minor

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

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
tpdServerPatchPendingAccept

Recovery

1. Accept or reject the patch per the application documentation procedure.

32540 - CPU Power limit mismatch

Alarm Group:
PLAT

Description:
The BIOS setting for CPU Power Limit is different than expected.

Severity:
Minor

Instance:
N/A

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
tpdCpuPowerLimitMismatch

Alarm ID:
TKSPLATMI41

Recovery:

1. It is recommended to contact My Oracle Support.

32700 - Telco Switch Notification

Alarm Group:
PLAT

Description
Telco Switch Notification

Severity
Info

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

HA Score
Normal

Auto Clear Seconds
86400

OID
tpdTelcoSwitchNotification

Recovery:

1. It is recommended to contact My Oracle Support.

32701 - HIDS Initialized

Alarm Group:
PLAT

Description:
This alarm indicates HIDS was initialized.

Default Severity:
Info

OID:
tpdHidsBaselineCreated

Recovery:

1. It is recommended to contact My Oracle Support.

32702 - HIDS Baseline Deleted

Alarm Group:
PLAT

Description:
HIDS baseline was deleted.

Default Severity:
Info

OID:
tpdHidsBaselineDeleted

Recovery:

1. It is recommended to contact My Oracle Support.

32703 - HIDS Enabled

Alarm Group:
PLAT

Description:
HIDS was enabled.

Default Severity:
Info

OID:
tpdHidsEnabled

Recovery:

1. It is recommended to contact My Oracle Support.

32704 - HIDS Disabled

Alarm Group:
PLAT

Description:
HIDS was disabled.

Default Severity:
Info

OID:
tpdHidsDisabled

Recovery:

1. It is recommended to contact My Oracle Support.

32705 - HIDS Monitoring Suspended

Alarm Group:
PLAT

Description:
HIDS monitoring suspended.

Default Severity:
Info

OID:
tpdHidsSuspended

Recovery:

1. It is recommended to contact My Oracle Support.

32706 - HIDS Monitoring Resumed

Alarm Group:
PLAT

Description:
HIDS monitoring resumed.

Default Severity:
Info

OID:
tpdHidsResumed

Recovery:

1. It is recommended to contact My Oracle Support.

32707 - HIDS Baseline Updated

Alarm Group:
PLAT

Description:
HIDS baseline updated.

Default Severity:
Info

OID:
tpdHidsBaselineUpdated

Recovery:

1. It is recommended to contact My Oracle Support.

DM-IWF (33000-33024)

This section provides information and recovery procedures for **DM-IWF**) alarms and events, ranging from 33000 to 33024, and lists the type 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 the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the **Alarms & Events** > **View History** page.

33000 - MAP-to-Diameter Service Registration Failure on DA-MP

Alarm Group:
DIWF

Description:
DM-IWF application was unable to register for MAP-to-Diameter transaction service. No MAP-to-Diameter transactions can be routed to this DA-MP.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppComagentProviderRegistrationFailureNotify

Recovery:

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

33001 - Diameter-to-MAP Service Registration Failure on DA-MP

Alarm Group:
DIWF

Description:
DM-IWF application was unable to register for Diameter-to-MAP transaction service. Diameter-to-MAP transactions cannot be serviced by this DA-MP.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppComagentUserRegistrationFailureNotify

Recovery:

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

33002 - DM-IWF DA-MP not associated with a Place

Alarm Group:
DIWF

Description:
DM-IWF DA-MP server is not associated with an AppWorks Place.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppServerPlaceFailureNotify

Recovery:

1. If the server is not associated with an AppWorks place, Admin Disable DM-IWF on the DA-MP server, add the server to an appropriate AppWorks Place, and then Admin Enable DM-IWF on the DA-MP server.
2. It is recommended to contact My Oracle Support for further assistance.

33003 - Insufficient memory for DM-IWF

Alarm Group:
DIWF

Description:
DA-MP does not have sufficient memory to support DM-IWF

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppInsufficientMemoryFailureNotify

Recovery:

1. If the VM:Database DA-MP profile is applied to the DA-MP (**Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**), verify that the DA-MP has at least 24GB of physical memory.
2. If the G6:Database or G6:Session DA-MP profile is applied to the DA-MP (**Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**), verify that the DA-MP has at least 48GB of physical memory.
3. If the G7:Database, G8:Database, G7:Session or G8:Session DA-MP profile is applied to the DA-MP (**Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**), verify that the DA-MP has at least 64GB of physical memory.
4. If the DA-MP does not have sufficient physical memory to support a profile, it is recommended to contact My Oracle Support for further assistance on how to upgrade memory.

33004 - DM-IWF Transaction Response Queue Utilization

Alarm Group:
DIWF

Description:
The DM-IWF Transaction Response Queue Utilization is approaching its maximum engineered capacity.

Severity:
Minor, Major, Critical

Instance:
RxDmiwfTranRspMsgQueue, DM-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppTransactionResponseQueueUtilizationNotify

Recovery:

1. This alarm should not normally occur when no other congestion alarms are asserted. If no additional congestion alarms are asserted, the DSR Application Task might be experiencing a problem that is preventing it from processing message from its transaction response queue. Examine the Alarm log in **Alarms & Events**.
2. It is recommended to contact My Oracle Support for assistance.

33005 - DM-IWF PTR Pool Utilization

Alarm Group:
DIWF

Description:
The DM-IWF PTR Pool Utilization is approaching its maximum engineered capacity. DM-IWF allocates a pending transaction record (PTR) for every pending Diameter-to-MAP and MAP-to-Diameter transaction. 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:
RxDmiwfTranRspMsgQueue, DM-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppPTRPoolUtilizationNotify

Recovery:

1. Examine the Alarm log in Alarms & Events and evaluate whether the DSR Application Task might be experiencing a problem processing the messages. The rate of messages being processed by DM-IWF can be monitored from the from **Status & Manage** > **KPIs** page
2. If one or more DA-MPs in a server site have failed, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DA-MP server status can be monitored from the **Status** > **Manage** > **Server**.
3. If one or more DM-IWF instances configured in a server site are unable to provide service, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DM-IWF application admin state can be monitored from **Diameter** > **Maintenance** > **Applications**. DM-IWF service provider status can be monitored from **Communication Agent** > **Maintenance** > **Routed Services Status**
4. If the problem persists, it is recommended to contact My Oracle Support.

33006 - MD-IWF Service Congestion

Event Group:
DIWF

Description:
DM-IWF could not forward a Request to MD-IWF due to MD-IWF Service Congestion.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfServiceCongestedNotify

Recovery:

1. The number of SS7-MPs that act as providers for the MAP Routed Service might be insufficient to service the offered ingress load. MAP Routed Service ("MDIWFSvc") provider status can be monitored from **Communication Agent** > **Maintenance** > **Routed Services Status**.

2. If the problem occurs frequently, it is recommended to contact My Oracle Support.

33007 - MD-IWF Error

Event Group:
DIWF

Description:
DM-IWF received notification indicating ComAgent Error/Timeout or MD-IWF Application generated Failure Response.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfErrorNotify

Recovery:

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

33008 - DM-IWF maximum pending transactions allowed exceeded

Event Group:
DIWF

Description:
DM-IWF rejected either a Diameter-to-MAP or MAP-to-Diameter transaction because it was unable to allocation a pending transaction record (PTR) for the transaction. DM-IWF allocates a PTR for every pending Diameter-to-MAP and MAP-to-Diameter transaction. 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:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDmiwfMaxPendTransactionsAllowedExceededNotify

Recovery:

1. Examine the Alarm log in Alarms & Events a evaluate whether the DSR Application Task might be experiencing a problem processing the messages. The rate of messages being processed by DM-IWF can be monitored from the from **Status & Manage** > **KPIs** page
2. If one or more DA-MPs in a server site have failed, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DA-MP server status can be monitored from the **Status & Manage** > **Server**.
3. If one or more DM-IWF instances configured in a server site are unable to provide service, this may result in too much traffic being forwarded to the DM-IWF instance reporting this alarm. DM-IWF application admin state can be monitored from **Diameter** > **Maintenance** > **Applications**. DM-IWF service provider status can be monitored from **Communication Agent** > **Maintenance** > **Routed Services Status**
4. If the problem persists, it is recommended to contact My Oracle Support.

33009 - DM-IWF unexpected Answer response received from a SS7-MP

Event Group:
DIWF

Description:
No pending transaction was found for the Answer response received from SS7-MP. When a Request message is forwarded to an SS7-MP, DM-IWF creates a pending transaction record (PTR). The PTR is abandoned if an Answer response is not received in a timely fashion.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDmiwfUnexpectedAnswerRspReceivedFromSS7MPNotify

Recovery:

1. If this event is occurring frequently, the MAP Response Timeout may be set too low. The MAP Response Timeout value can be reviewed via **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options** screen.
2. If the problem persists, it is recommended to contact My Oracle Support.

33010 - MD-IWF ComAgent Connection exhausted

Event Group:
DIWF

Description:
DM-IWF failed to receive a Diameter Answer in response to a Diameter Request that was forwarded to MD-IWF Routed Service, in a timely fashion.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDmiwfMapComAgentConnectionExhaustedNotify

Recovery:

1. If this event is occurring frequently, the MAP Response Timeout may be set too low. The MAP Response Timeout value can be reviewed via **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options** screen.
2. If the problem persists, it is recommended to contact My Oracle Support.

33011 - DM-IWF Answer Timeout

Event Group:
DIWF

Description:
DM-IWF failed to receive a Diameter Answer in response to a Diameter Request that was forwarded to **MD-IWF** Routed Service, within the DM-IWF Pending Answer Timer expiration.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDmiwfAnswerTimeoutNotify

Recovery:

1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. It's possible that the MAP Origination Transaction Timer value is set too low. The MAP Origination Transaction Timer value setting can be viewed via the following GUI screen: **MAP Interworking** > **Configuration** > **Options (MD-IWF tab)**.
2. If the problem persists, it is recommended to contact My Oracle Support.

33012 - DM-IWF encode decode error

Event Group:
DIWF

Description:
The decoder has reported an error causing the Request to be discarded.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDmiwfDecodeErrorNotify

Recovery:

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

33013 - DRL queue exhaustion

Event Group:
DIWF

Description:
DM-IWF failed to forward a Diameter message to DRL due to DRL queue exhaustion.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDrlQueueExhaustionNotify

Recovery:

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

> **Note:** This measurement should not occur unless the MP is experiencing local congestion as indicated by Alarms 22000 - Local MP Congestion, 22201 - Ingress Message Rate, 22204 - Request Message Queue Utilization, and 22205 - Answer Message Queue Utilization. Refer to the *DSR Alarms and KPIs Reference* for details about these alarms.

33014 - Incompatible DA-MP Profile for DM-IWF

Alarm Group:
DIWF

Description:
DA-MP has been assigned a profile that is incompatible with DM-IWF

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterDmiwfAppIncompatibleProfileFailureNotify

Recovery:

1. If the DA-MP has been assigned a DA-MP profile (**Diameter** > **Configuration** > **DA-MPs** > **Profile Assignments**) other than those listed below, apply a compatible profile and restart DSR (**Status & Manage** > **Server** > **Restart**.
   - G6:Database
   - G7:Database
   - G8:Database
   - VM:Database

- G6:Session
- G7:Session
- G8:Session

2. If the DA-MP has been assigned a compatible profile and the problem persists, contact My Oracle Support for assistance.

33015 - DM-IWF Diameter message size exceeded maximum supported size

Event Group:
DIWF

Description:
DM-IWF failed to forward the Diameter message to SS7-MP because the message size exceeds supported maximum message size.

Severity:
Info

Instance:
<DAMPName>

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterDmiwfMaxDiameterMsgSizeExceededNotify

Recovery:

1. Occurrence of this event indicates that diameter message received has size that exceeds maximum diameter message size supported by MAP-Diameter Interworking function and therefore be handled as "Internal Processing Error". Source of these requests can be tracked using "Origin Host", "Application Id" and "Command Code".

MD-IWF (33050-33099)

This section provides information and recovery procedures for **MD-IWF** alarms and events, ranging from 33050 to 33099, and lists the type 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 the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the **Alarms & Events** > **View History** page.

33050 - MD-IWF Ingress Message Rate

Alarm Group:
MIWF

Description:
The ingress message rate for the MD-IWF Application is approaching or exceeding its engineered traffic handling capacity.

Severity:
Minor, Major, Critical

Instance:
RxMdIwfIngressMsgRate, MD-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfIngressMsgRateNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Diameter** > **Configuration** > **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 from **Status & Manage** > **KPIs**. If 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 further assistance.

33051 - MD-IWF Application Degraded or Unavailable

Alarm Group:
MIWF

Description:
MD-IWF Application operational status is Degraded or Unavailable.

Severity:
Major, Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfApplDegradedOrUnavailableNotify

Recovery:

1. An MD-IWF Application operational status becomes Degraded when either the Admin State is set to disabled with the forced shutdown option or the Admin State is set to disabled with the graceful shutdown option and the graceful shutdown timer expires.
2. The MD-IWF Application can also become Degraded when it reaches Congestion Level 1, 2, or 3 if enabled.

   Note: This alarm will NOT be raised when the MD-IWF application is shutting down gracefully or application is in Disabled state. Only the MD-IWF Application operational status will be changed to Unavailable.

3. An MD-IWF Application operational status becomes Unavailable when either the Admin State is set to disabled with the forced shutdown option or the Admin State is set to disabled with the graceful shutdown option and the graceful shutdown timer expires.
4. The MD-IWF Application can also become Unavailable when it is isolated from the SS7 network.

   Note: This alarm will NOT be raised when the MD-IWF application is shutting down gracefully or application is in Disabled state. Only the MD-IWF Application operational status will be changed to Unavailable.

5. Monitor the MD-IWF Application status can be monitored from **Diameter** > **Maintenance** > **Applications**. Verify the admin state is set as expected.
6. Check the event history logs for additional events or alarms from this SS7-MP server.
7. If the problem persists, it is recommended to contact My Oracle Support.

33052 - MD-IWF Notified that DM-IWF Service Status is Down

Alarm Group:
MIWF

Description:
The MD-IWF is notified via ComAgent that the rolled-up DM-IWF Service Status is Down.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfUserSvcDownNotify

Recovery:

1. Investigate the status of all DA-MP servers. As this status is a rolled-up status, it indicates that no DA-MP servers are able to be a provider of the DM-IWF ComAgent Routed Service.
2. It is recommended to contact My Oracle Support for further assistance.

33053 - MD-IWF DiamTrans Task Queue Utilization

Alarm Group:
MIWF

Description:
The MD-IWF Application DiamTrans Task Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
RxMdIwfDiamTransMsgQueue (TaskID), MD-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfDiamTransQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Diameter** > **Configuration** > **Application Route Tables**.
2. If no additional congestion alarms are asserted, the MD-IWF Application Task may be experiencing a problem preventing it from processing messages from its DiamTrans Task Queue. Examine the alarm log from **Alarms & Events**.
3. It is recommended to contact My Oracle Support for further assistance.

33054 - MD-IWF MapTrans Task Queue Utilization

Alarm Group:
MIWF

Description:
The MD-IWF Application MapTrans Task Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
RxMdIwfMapTransMsgQueue (TaskId), MD-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfMapTransQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Diameter** > **Configuration** > **Application Route Tables**.
2. If no additional congestion alarms are asserted, the MD-IWF Application Task may be experiencing a problem preventing it from processing messages from its DiamTrans Task Queue. Examine the alarm log from **Alarms & Events**.
3. It is recommended to contact My Oracle Support for further assistance.

33055 - MD-IWF DAMPInterface Task Queue Utilization

Alarm Group:
MIWF

Description:
The MD-IWF Application DAMPInterface Task Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
RxMdIwfDampInterfaceMsgQueue, MD-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfDampInterfaceQueueUtilNotify

Recovery:

1. The Application Routing Table may be mis-configured and sending too much traffic to the DM-IWF DSR Application. Verify the configuration via **Diameter** > **Configuration** > **Application Route Tables**.

2. If no additional congestion alarms are asserted, the MD-IWF Application Task may be experiencing a problem preventing it from processing messages from its DAMPInterface Task Queue. Examine the alarm log from **Alarms & Events**.
3. It is recommended to contact My Oracle Support for further assistance.

33056 - MD-IWF ComAgent Provider Registration Failure on SS7-MP

Alarm Group:
MIWF

Description:
MD-IWF Application was unable to register with ComAgent as a provider of the MDIWFSvc service. No Diameter-to-MAP transactions can be routed to this SS7-MP.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfComAgentProviderRegisFailureNotify

Recovery:

1. It is recommended to contact My Oracle Support for further assistance.

33057 - MD-IWF ComAgent User Registration Failure on SS7-MP

Alarm Group:
MIWF

Description:
MD-IWF application was unable to register with **ComAgent** as a user of the DMIWFSvc service. MAP-to-Diameter transactions cannot be processed by this SS7-MP.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfComAgentUserRegisFailureNotify

Recovery:

1. It is recommended to contact My Oracle Support for further assistance.

33058 - MD-IWF DiamToMap PTR Utilization

Alarm Group:
MIWF

Description:
The MD-IWF Application DiamToMap PTR Utilization is approaching its maximum engineered capacity.

Severity:
Minor, Major, Critical

Instance:
EvMdIwfDiam2MapPtrUtil, MD-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfDiamToMapPtrUtilNotify

Recovery:

1. A DiamToMap PTR is allocated for every pending Diameter-to-Map transaction. The PTR size is engineered based on an average transaction holding size. If the PTRs becomes depleted, no new transactions can be processed by the MD-IWF application.
2. PTR exhaustion is most likely caused by long delays in the Diameter or SS7 networks. PTR exhaustion problems can be reduced/eliminated by reducing the MAP timer values.
3. View the current MAP timers from **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.
4. It is recommended to contact My Oracle Support for further assistance.

33059 - MD-IWF MapToDiam PTR Utilization

Alarm Group:
MIWF

Description:
MD-IWF Application MapToDiam PTR Utilization is approaching its maximum engineered capacity.

Severity:
Minor, Major, Critical

Instance:
EvMdIwfMap2DiamPtrUtil, MD-IWF

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfMapToDiamPtrUtilNotify

Recovery:

1. A MapToDiam PTR is allocated for every pending MAP-to-Diameter transaction. The size of the PTR size is engineered based on an average transaction holding size. If the PTRs become depleted, no new transactions can be processed by the MD-IWF application.
2. Determine if there are long delays in the Diameter or SS7 networks. PTR pool exhaustion can be reduced or eliminated by reducing the MAP timer values.
3. The current MAP timers can be viewed in the GUI at **MAP Interworking** > **Configuration** > **MD-IWF Options**.
4. It is recommended to contact My Oracle Support for further assistance.

33060 - SS7-MP Profile Not Assigned

Alarm Group:
MIWF

Description:
An SS7-MP configuration profile has not been assigned to this SS7-MP

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterSs7MpProfileNotAssignedNotify

Recovery

1. If the SS7-MP has been assigned an MP Profile from an SO GUI **Diameter Common** > **MPs** > **Profile Assignment** other MD-IWF, apply a compatible profile and restart the mapiwf process from **Status & Manage** > **Server**.
2. If the SS7-MP has been assigned a compatible profile already, it is recommended to contact My Oracle Support for further assistance.

33062 - Insufficient Memory for MD-IWF

Alarm Group:
MIWF

Description:
SS7-MP does not have sufficient memory to support MD-IWF.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfInsufficientMemoryForMdiwfNotify

Recovery

1. If MD-IWF was mistakenly activated, deactivate MD-IWF.
2. If the SS7-MP does not have sufficient physical memory, upgrade the memory.
3. It is recommended to contact My Oracle Support for further assistance.

33063 - MD-IWF SS7-MP not associated with a Place

Alarm Group:
MIWF

Description:
The MD-IWF SS7-MP server is not associated with an AppWorks Place.

Severity:
Critical

Instance:
None

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterMdIwfSs7MpNotAssocWithPlaceNotify

Recovery

1. Set the MD-IWF admin state to Disabled on the SS7-MP server.
2. If the server is not associated with an AppWorks place, add the server to an appropriate AppWorks Place. Then set the MD-IWF admin state to Enabled on the SS7-MP server.
3. It is recommended to contact My Oracle Support for further assistance.

33065 - MD-IWF Resource Exhaustion

Event Group:
MIWF

Description:
MD-IWF Application is unable to process a message due to resource exhaustion.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Auto Clear Seconds:
300 seconds (5 minutes)

OID:
eagleXgDiameterMdIwfResourceExhaustionNotify

Recovery

1. Check to see if any of the following resource utilization alarms are present on the SS7-MP. If so, follow the steps specified for the given alarm.
   - 33053 - MD-IWF DiamTrans Task Queue Utilization
   - 33054 - MD-IWF MapTrans Task Queue Utilization
   - 33055 - MD-IWF DAMPInterface Task Queue Utilization
   - 33058 - MD-IWF DiamToMap PTR Utilization
   - 33059 - MD-IWF MapToDiam PTR Utilization
   - 22202 - MpDiamMsgPoolCongested
2. It is recommended to contact My Oracle Support for assistance if needed.

33066 - MD-IWF orphan Diameter Answer message received

Event Group:
MIWF

Description:
MD-IWF Application received a Diameter Answer message for which no Pending Transaction record exists.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfOrphanDiamAnswerNotify

Recovery

1. When MD-IWF sends a Diameter Request message to a DA-MP, it allocates a PTR and starts a timer (value is user configurable). The pending transaction is abandoned if a Diameter Answer response is not received within the user-configurable time limit. If this event is occurring frequently, the timer may be set too low. The Diameter Response Timeout value can be viewed via the **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options** NO GUI Screen.
2. It is recommended to contact My Oracle Support for assistance if needed.

33067 - MD-IWF orphan MAP Response message received

Event Group:
MIWF

Description:
MD-IWF Application received a MAP response message for which no Pending Transaction record exists.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfOrphanMapResponseNotify

Recovery

1. If this event is occurring frequently, the configurable MAP Response timer may be set too low. The MAP Response Timeout value can be viewed via the NO GUI **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.
2. It is recommended to contact My Oracle Support for assistance if needed.

33068 - MD-IWF MAP Response timeout

Event Group:
MIWF

Description:
MD-IWF Application sent a MAP request message to the SS7 network, but timed out waiting for the MAP response.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfMapResponseTimeoutNotify

Recovery

1. Diameter-to-MAP timeouts are most likely caused by excessive SS7 network delays. It is possible that the MAP Response Timeout value is set too low.
2. The configured MAP Response Timeout value can be viewed via **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.
3. It is recommended to contact My Oracle Support for assistance if needed.

33069 - MD-IWF Diameter Answer timeout

Event Group:
MIWF

Description:
MD-IWF Application sent a Diameter Request message to the DA-MP, but timed out waiting for the Diameter Answer.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfDiamAnswerTimeoutNotify

Recovery

1. MAP-to-Diameter timeouts could be caused by delays in the Diameter network. It is possible that the Diameter Response Timeout value is set too low.
2. The configured Diameter Response Timeout value can be viewed via the NO GUI **MAP-Diameter IWF** > **Configuration** > **MD-IWF Options**.
3. It is recommended to contact My Oracle Support for assistance if needed.

33070 - MD-IWF Generated Diameter Answer error message due to Diameter Exception

Event Group:
MIWF

Description:
An error occurred while MD-IWF Application was processing a Diameter Request message, causing it generate a Diameter Answer error message.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfGeneratedDiamErrorAnswerNotify

Recovery

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

33071 - MD-IWF Generated MAP Error Response due to MAP exception

Event Group:
MIWF

Description:
An error occurred while MD-IWF Application was processing a MAP request message, causing it generate a MAP response error message.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfGeneratedMapErrorResponseNotify

Recovery

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

33072 - MD-IWF received TCAP Notice from SS7 network

Event Group:
MIWF

Description:
MD-IWF Application received a TCAP Notice from the SS7 network.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfTcapNoticeRecdNotify

Recovery

1. A TC-Notice informs the TCAP Application that the network service provider is unable to provide the requested service.

33073 - MD-IWF admin state set to Enabled

Event Group:
MIWF

Description:
MD-IWF Application admin state was changed to Enabled on the SS7-MP

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfAdminStateEnabledNotify

Recovery

1. No action required.

33074 - MD-IWF admin state set to Disabled

Event Group:
MIWF

Description:
MD-IWF Application admin state was changed to Disabled on the SS7-MP

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfAdminStateDisabledNotify

Recovery

1. No action required.

33075 - MD-IWF received ComAgent error or DM-IWF NACK

Event Group:
MIWF

Description:
MD-IWF sent a Diameter Request message to DM-IWF that resulted in a ComAgent error / timeout or in a DM-IWF NACK.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfRcvdComAgtErrorOrDmiwfNckNotify

Recovery

1. No action required.

33076 - MD-IWF received Diameter Anwer from unexpected DA-MP

Event Group:
MIWF

Description:
MD-IWF received Diameter Answer from unexpected DA-MP

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfDiamAnsRcvdFrmUnexcpDaMpNotify

Recovery

1. This error is not expected to occur. It is recommended to contact My Oracle Support for assistance if needed.

33077 - MD-IWF address translation failed

Event Group:
MIWF

Description:
MD-IWF was not able to perform address translation due to a lookup error in a configuration table, or else due to a missing or unexpected parameter/AVP.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfAddressTranslationFailedNotify

Recovery

1. If address translation failed due to a lookup error in a configuration table, then analyze the configuration table to see if there is missing or incorrect data.
2. If address translation failed due to missing or unexpected MAP parameter or Diameter AVP value, then analyze the message to see if it is correct.
3. It is recommended to contact My Oracle Support for assistance if needed.

33078 - MD-IWF received Diameter EIR message but Destination-Host AVP not present or not found in mapping table

Event Group:
MIWF

Description:
MD-IWF Application received a Diameter EIR message but the Destination-Host AVP was either 1) not present or 2) the Destination-Host AVP value was not present in table DiamIdentityGta.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfDiamEirRecdDestHostNotPresentNotify

Recovery

1. For case 1, investigate why the Destination-Host AVP was not present in the message. The DSR expects this AVP to be present.
2. For case 2, check to see if table DiamIdentityGta is configured correctly. It is possible the given Destination Host should be present in this table. This table is configured on the NO GUI via **MAP-Diameter IWF** > **Configuration** > **Diameter Identity GTA**.
3. It is recommended to contact My Oracle Support for assistance if needed.

33079 - MD-IWF message translation failed

Event Group:
MIWF

Description:
MD-IWF attempt to perform message translation was unsuccessful.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfMessageTranslationFailedNotify

Recovery

1. Based on the Translation Error Details, examine the message being translated and attempt to identify the reason for the failure
2. It is recommended to contact My Oracle Support for assistance if needed.

33080 - EDL failure occurred while MD-IWF attempted to encode a Diameter message

Event Group:
MIWF

Description:
EDL failure occurred while MD-IWF attempted to encode a Diameter message.

Severity:
Info

Instance:
mapiwf

HA Score:
Normal

Throttle Seconds:
10

OID:
eagleXgDiameterMdIwfDiamEirRecdDestHostNotPresentNotify

Recovery

1. Examine the EDL error text in order to determine the reason for failure, If the encode failure is due to exceeding the maximum supported Diameter message size, and this event is being raised frequently, then it may be necessary to increase the engineering configurable parameter (DiameterMaxMessageSize in table MapIwfLongConfig) for maximum Diameter message size.
2. It is recommended to contact My Oracle Support for assistance if needed.

GLA (33100-33149)

This section provides information and recovery procedures for **GLA** alarms and events, ranging from 33100 to 33149, and lists the type 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 the Launch Alarms Dashboard GUI menu option. The alarms and events log can be viewed from the **Alarms & Events** > **View History** page.

33100 - GLA Message Decoding Failure

Event Group:
GLA

Description:
Message received was rejected because of a decoding failure.

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaMessageDecodingFailureNotify

Recovery:

1. While parsing the message, one of the following conditions occurred:
   - The message content was inconsistent with the "Message Length" in the message header.
   - The IMSI contained in the User-Name AVP was considered invalid due to length.
   - The MSISDN contained in the MSISDN AVP was considered invalid due to length.
2. These protocol errors 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. Collect a trace containing the GGR, and determine which node is causing the invalid data.
3. If the problem persists, it is recommended to contact My Oracle Support.

33101 - GLA Incorrect Application ID or Command Code

Event Group:
GLA

Description:
Message received was rejected because the Application ID was not GL (16777321) or the Command Code was not GGR (8388655).

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaIncorrectApplIdOrCmdCodeNotify

Recovery:

1. Examine the Application Routing Rules that direct traffic to GLA and verify that the Application ID is set to GL (16777321) and the Command Code is set to GGR (8388655) for all Application Routing Rules referring to GLA.

33102 - GLA Missing Subscriber ID

Event Group:
GLA

Description:
Message received was rejected because it did not contain and IMSI or an MSISDN in a Subscription-ID AVP.

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaMissingSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.
2. If this condition is met, inspect each element between the **GQC** and **GWS** to determine if Subscriber information within the Request is being modified.

33103 - GLA Communication Agent Error

Event Group:
GLA

Description:
GLA was unable to communicate with the pSBR-Binding due to a communications error.

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaComAgentErrorNotify

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.
2. Examine the status of the Reporting server's BindingRd to verify that all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, it is recommended to contact My Oracle Support.

33104 - GLA Duplicate Subscriber ID

Event Group:
GLA

Description:
Message received was rejected because it contained both a User-Name AVP and a MSISDN AVP

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaDuplicateSubscriberIdNotify

Recovery:

1. Verify that the Originator (identified by the Origin-Host AVP in the message) is generating Diameter Requests with either User-Name AVP or MSISDN AVP being present.
2. Inspect each element between teh GQC and GQS to determine which node is inserting bot AVPs and correct that node so that only one AVP is included in the GGR.

33105 - Routing Attempt failed due to queue exhaustion

Event Group:
GLA

Description:
Message could not be routed because the internal "Answer Message Queue" to the DSR Relay Agent was full.

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaRoutingAttemptFailureDrlQueueExhNotify

Recovery:

1. This condition should not occur unless the DSR is experiencing severe congestion due to excessive traffic levels arriving on the DRL Answer Queue.
2. GL traffic should be diverted from the DA-MP to other DA-MPs in the DSR, or to another DSR.

33106 - GLA Communication Agent Timeout

Event Group:
GLA

Description:
GLA was unable to communicate with the pSBR-Binding and the query timed out.

Severity:
Info

Instance:
"MP"

HA Score:
Normal

Throttle Seconds:
60

OID:
eagleXgDiameterGlaComAgentTimeoutNotify

Recovery:

1. Examine the current state of the pSBR-B via the **Communication Agent** > **Maintenance** > **HA Service Status** screen.

2. Examine the status of the Reporting server's BindingRd to verify all SubResources are Available. This action will provide information about Availability and Congestion of each SubResource.
3. If the problem persists, it is recommended to contact My Oracle Support.

33120 - Policy SBR Binding Sub-Resource Unavailable

Alarm Group:
GLA

Description:
GLA is unable to communicate with Policy SBR-Binding. One or more binding sub-resources are unavailable.

Severity:

- Major: When at least one server group that has a range of binding sub-resources is not available, but at least the minimum number of binding sub-resources is still available.
- Critical: When fewer than the minimum number of binding sub-resources are not available.

Instance:
GLA

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterGlaBindingSubresourceUnavailableNotify

Recovery

1. Monitor the Policy DRA Binding Resource on the GLA NO at **Configuration** > **Resource Domains**.
2. Determine if some of the pSBR-B MPs are unavailable or out-of-service. In this case, all DA-MPs and all pSBR-B MPs will also report ComAgent connection alarms.
3. Determine if there is a WAN outage. In this case, DA-MPs should also report ComAgent connection alarms to remote pSBR-Bs, and local pSBR-Bs should report ComAgent connection alarms to remote DA-MPs.
4. Determine if there is a network routing issue. In this case, one or a few DA-MPs may report a ComAgent connection against a limited number of pSBR-Bs.
5. If the problem persists, it is recommended to contact My Oracle Support for assistance.

33121 - GLA pSBR-B Response Task Message Queue Utilization

Alarm Group:
GLA

Description:
GLA's pSBR-B Response Message Queue Utilization is approaching its maximum capacity.

Severity:
Minor, Major, Critical

Instance:
RxGlaResponseMsgQueue, GLA

HA Score:
Normal

Auto Clear Seconds:
0 (zero)

OID:
eagleXgDiameterGlaRespTaskMessageQueueUtilizationNotify

Recovery

1. Determine if the GLA pSBR Response Task is mis-configured (e.g., Smaller response task queue size/fewer number of response task threads as compared to the request task threads).
2. Determine if the GLA pSBR Response Task has encountered a problem preventing it from processing messages from its Task Message Queue even if no additional congestion alarms are asserted.
3. If the problem persists, it is recommended to contact My Oracle Support for additional assistance.

Diameter Custom Applications (DCA) Framework Alarms and Events (33300-33630)

This section provides information and recovery procedures for differentiated DCA Framework alarms, which range from 33300 to 33630.

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

Recovery

1. 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

Recovery

1. 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

Recovery

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

33303 - U-SBR Event Queue Utilization

Alarm Group
DCA

Description
The DSR Application U-SBR Event Queue Utilization is approaching its maximum capacity.

Severity
Minor, Major, Critical

Instance
RxDcaSbrEventMsgQueue [<*DcaDalId.dalId*>], DCA

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
dcaDSRAppSbrEventMessageQueueUtilizationNotify

Recovery

1. The DSR Application's U-SBR 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 U-SBR results by the DCA app indicate that the DCA app is overly CPU-intensive. The alarm may also be the result of the DCA app sending too many U-SBR queries per Diameter message, which may be avoided by storing variables in the Diameter transaction context. In both cases the business logic shall be reviewed and optimized.

   If no additional congestion alarms are asserted, the DSR Application Task may be experiencing a problem preventing it from processing messages from its U-SBR Event Message Queue. Examine the alarm log from **Alarms & Events**.

2. 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

Recovery

1. 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 SBR Event)

HA Score
Normal

Auto Clear Seconds
60

OID
dcaDSRAppProcedureNotFoundNotify

Recovery

1. 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** > **DCA Framework** > **<Application Name>** > **General Options** on the NOAM) or the callback names coded in the Perl script.

   Possible resolutions are:

   a. Fix the procedure names in the Perl script and re-compile the Perl script

   b. Fix the procedure names in the configuration

   c. 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.

33306 - U-SBR Resolution Failure

Alarm Group
DCA

Description
The U-SBR DB logical name could not be resolved to a physical U-SBR DB.

Severity
Critical

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
dcaDSRAppUsbrResFailureNotify

Recovery

1. This alarm occurs because the L2P mapping for a DCA Application is incomplete in the sense that none of the physical U-SBR DBs provisioned (for one or more logical U-SBR DBs) is located in the same Place Association with the MP that raises the alarm.
2. Ensure that a physical U-SBR DB has been configured for each Place Association and that all the physical U-SBR DBs have been included in the L2P mapping by checking:
   - **Main Menu** > **DCA** > **<DCA Application Name>** > **Application Control** > **<Version Name>** > **SBR Database Name Mapping** (on the NOAM)
   - **Main Menu** > **Session Binding Repository** > **Configuration** > **SBR Databases**

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

Recovery

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

33308 - DCA to U-SBR ComAgent Error

Event Type
DCA

Description
DCA failed to send query to U-SBR 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

Recovery

1. 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

Recovery

1. 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.

33310 - U-SBR Sub-resource Unavailable

Alarm Group
DCA

Description
One or more U-SBR server groups hosting a U-SBR DB are unavailable.

Severity
Major, Critical

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:" and the U-SBR DB logical name (*DcaLogicalSbr.logSbrDb*)

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
dcaDSRSubresourceUnavailableNotify

Recovery

1. Monitor U-SBR resources at **Configuration** > **Resource Domains**.
2. It is recommended to contact My Oracle Support for assistance.

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

Recovery

1. 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

Recovery

1. Ensure that enough space is available on the partition where `/tmp/appworks_temp` resides and re-initiate the script compilation.

33313 - DCA U-SBR Logical Name Mismatch

Alarm Group
DCA

Description
No mapping has been provisioned for the U-SBR logical name.

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
dcaDSRUsbrLogicalNameErrorNotify

Recovery

1. Fix either the logical U-SBR name in the script or the Logical-to-Physical U-SBR DB names mapping (**Main Menu** > **DCA Framework** > **<Application Name>** > **Application Control** > **<Version Name>** > **SBR Database Name Mapping** on the NOAM). The physical U-SBR DBs configured in the network are listed in **Main Menu** > **SBR** > **Configuration** > **SBR Databases**. The script must be recompiled.

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.

33314 - Custom MEAL differentiation error

Alarm Group
DCA

Description
The differentiation, un-differentiation, or update process of a Custom MEAL has been interrupted and will be retried in 10 seconds

Severity
Minor

Instance
The DCA App short name (*DcaDalId.shortName*) prefixed with "DCA:"

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
DcaCustomMealDiffErrorNotification

Recovery

1. If the alarm does not clear on its own, it is recommended to contact My Oracle Support for assistance.

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*

33430-33479 - 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

Recovery

1. 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

Recovery

1. If total active session bindings fall below the clear threshold, this alarm clears.
2. Navigate to **CPA** > **Configuration** > **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
sbrProcTerm

Recovery

1. 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.

   a. Check the status of the terminated SBR by navigating to **Status & Manage** > **Server**.

   b. 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
uSBRAuditStatisticsReport

Recovery

1. 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 (70000-70999)

70000 - Association Down

Alarm Group
vSTP

Description
Association down

Severity
Major

Instance
<AssocName>

HA Score
Normal

Auto Clear Seconds
0 (zero)

OID
vSTPVstpassociationDownNotify

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** > **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

Recovery

1. If the association hosting the link or the link itself is manually disabled, then no further action is needed.
2. Verify alarm 70000 - Association Down is not raised for the association hosting the link. If the alarm is raised, refer to the recovery steps for that alarm.
3. Verify RCs are configured properly at associated linkset.
4. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
5. Verify that the remote ASP 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

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. Monitor the RSP/Destination at **SS7/SIGTRAN** > **Maintenance** > **Remote Signaling Points**.
4. Verify IP network connectivity exists between the MP server and the adjacent servers.
5. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
6. 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

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. Monitor the route status at **SS7/SIGTRAN** > **Maintenance** > **Remote Signaling Points**.
4. Verify IP network connectivity exists between the MP server and the adjacent servers.

5. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
6. 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

Recovery

1. M3UA attempts to automatically recover all links not manually disabled or blocked.
2. Monitor the Linkset status at **SS7/SIGTRAN** > **Maintenance** > **Linksets**.
3. Verify IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
5. Verify the adjacent server is not under maintenance.
6. 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

Recovery

1. M3UA attempts to automatically recover all links not manually disabled or blocked.
2. Monitor the Linkset status at **SS7/SIGTRAN** > **Maintenance** > **Links**.
3. Verify IP network connectivity exists between the MP server and the adjacent servers.
4. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
5. Verify that the adjacent server is not under maintenance.
6. 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

Recovery

1. Monitor the route status at **SS7/SIGTRAN** > **Maintenance** > **Remote Signaling Points**.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
4. Verify the adjacent server is not under maintenance.
5. 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

Recovery

1. Monitor the route status at **SS7/SIGTRAN** > **Maintenance** > **Remote Signaling Points**.
2. Verify IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
4. Verify the adjacent server is not under maintenance.
5. 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

Recovery

1. Monitor the route status at **SS7/SIGTRAN** > **Maintenance** > **Remote Signaling Points**.
2. Verify that IP network connectivity exists between the MP server and the adjacent servers.
3. Check the event history logs at **Alarms & Events** > **View History** for additional SS7 events or alarms from this MP server.
4. Verify that the adjacent server is not under maintenance.
5. 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

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** > **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** > **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** > **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

70050 - SCTP connection refused

Alarm Group
vSTP

Description
SCTP connection refused.

Severity
Info

Instance
<Link>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPSctpConnectionRefusedNotify

Recovery

1. 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

Event Group
vSTP

Description
Failed to configure Transport.

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPFailedtoconfigureConnectionNotify

Recovery

1. 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

Event Group
vSTP

Description
Far-end closed the connection

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPFarendclosedtheconnectionNotify

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

Event Group
vSTP

Description
SCTP connection closed

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPSctpconnectionclosedNotify

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** > **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

Event Group
vSTP

Description
Remote IP Address state change

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPRemoteIPAddressstatechangeNotify

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

Event Group
vSTP

Description
Association admin state change

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPAssociationadminstatechangeNotify

Recovery

1. 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

Event Group
vSTP

Description
Link admin state change

Severity
Info

Instance
<AssociationName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPLinkadminStateChangeNotify

Recovery

1. 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

Event Group
vSTP

Description
Received invalid M3UA message

Severity
Info

Instance
<AssociationName>, <LinkName>, or <LinkId>

HA Score
Normal

Throttle Seconds
10

OID
vSTPVstpReceivedinvalidM3UAMessageNotify

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 (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

Event 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

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 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

Event Group
vSTP

Description
Failed to send DITA message

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPMtp3TfpReceivedNotify

Recovery

1. Check the event history logs at **Alarms & Events** > **View History** for additional events or alarms from this MP server.
2. Verify that 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.

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

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** > **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** > **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** > **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

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

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

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

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** > **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** > **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** > **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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. 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

Recovery

1. The alarm is an indication of M3UA Tx Stack Event queue utilization is exceeding its configured capacity. It is recommended to contact My Oracle Support for assistance if needed

70201 - M2PA link operational state changed

Event Group
vSTP

Description
M2PA link operational state changed

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPLinkOpStateChangedNotify

Recovery

1. No action necessary

70202 - M2PA link failed

Event Group
vSTP

Description
M2PA link failed

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
0 (zero)

OID
vSTPLinkFailedNotify

Recovery

1. No action necessary

70203 - M2PA Ingress message discarded

Event Group
vSTP

Description
M2PA Ingress message discarded

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPIngressMessageDiscardedNotify

Recovery

1. No action necessary

70204 - M2PA Egress message discarded

Event Group
vSTP

Description
M2PA Egress message discarded

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPEgressMessageDiscardedNotify

Recovery

1. No action necessary

70205 - M2PA Message Encoding Failed

Event Group
vSTP

Description
M2PA Message Encoding Failed

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPMessageEncodeFailedNotify

Recovery

1. No action necessary

70206 - M2PA Message Decoding Failed

Event Group
vSTP

Description
M2PA Message Decoding Failed

Severity
Info

Instance
<LinkName>

HA Score
Normal

Throttle Seconds
10

OID
vSTPMessageDecodeFailedNotify

Recovery

1. No action necessary

70271 - SCCP Received Invalid Message

Event Group
vSTP

Description
SCCP Received Invalid Message

Severity
Info

Instance
None

HA Score
Normal

Throttle Seconds
10

OID
vSTPSccpInvalidMessageReceivedNotify

Recovery

1. No action necessary

70272 - SCCP Message Translation Failed

Event Group
vSTP

Description
SCCP Message Translation Failed

Severity
Info

Instance
None

HA Score
Normal

Throttle Seconds
10

OID
vSTPSccpTranslationFailedNotify

Recovery

1. No action necessary

70273 - SCCP Message Routing Failed

Event Group
vSTP

Description
SCCP Message Routing Failed

Severity
Info

Instance
None

HA Score
Normal

Throttle Seconds
10

OID
vSTPSccpMessageRoutingFailedNotify

Recovery

1. No action necessary

70274 - SGMG Message Invalid

Event Group
vSTP

Description
SGMG Message Invalid

Severity
Info

Instance
None

HA Score
Normal

Throttle Seconds
10

OID
vSTPScmgMessageInvalidNotify

Recovery

1. No action necessary

70275 - GTT SCCP Loop Detected

Event Group
vSTP

Description
GTT SCCP Loop Detected

Severity
Info

Instance
None

HA Score
Normal

Throttle Seconds
10

OID
vSTPGttSccpLoopDetectedNotify

Recovery

1. No action necessary

70276 - GTT Load Sharing Failed

Event Group
vSTP

Description
GTT Load Sharing Failed

Severity
Info

Instance
None

HA Score
Normal

Throttle Seconds
10

OID
vSTPGttLoadSharingFailedNotify

Recovery

1. No action necessary

5

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 > KPI page, and how to view KPIs.

KPIs overview

Key Performance Indicators (KPIs) allow you to monitor system performance data, including CPU, memory, swap space, 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** > **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 appear regardless of server role.

Table 5-1 KPIs Server Elements

KPIs Status Element	Description
Network Element	The network element name (set up on the **Configuration** > **Network Elements** page) associated with each Server Hostname.
Server Hostname	The server hostname set up on the **Configuration** > **Servers** page. All servers in the system are listed here.
Server Indicators:	

Table 5-1 (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.
Uptime	The total amount of time the server has been running.

Viewing KPIs

Use this procedure to view KPI data.

1. Select **Status & Manage** > **KPIs**.

   The Status & Manage > KPIs page appears with the **Server** tab displayed. For details about the KPIs displayed on this page, see the application documentation.

2. Click the **KPI Filter** button and specify filter options using the drop-down menus 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 5-2 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

Table 5-2 (Cont.) Schedule KPI 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.
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.

Use this procedure to schedule a data export task.

1. Select **Status & Manage** > **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** > **Files** page, you can view a list of files available for download, including the file you exported during this procedure. For more information, see Viewing the file list.

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

   - Viewing scheduled tasks
   - 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** > **KPIs**.

Table 5-3 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.

Table 5-3 (Cont.) CAPM KPIs

Variable	Description
Match Rule	References one element in the arrayed measurement.

Communication Agent (ComAgent) KPIs

The KPI values associated with **ComAgent** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-4 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.

Diameter (DIAM) KPIs

The KPI values associated with **Diameter** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-5 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.

DM-IWF KPIs

The KPI values associated with DM-IWF are visible using **Status & Manage** > **KPIs**

Table 5-6 DM-IWF KPIs

Variable	Description
Ingress Msg Rate	Average number of MAP-Diameter Interworking messages processed per second on a DA-MP. This includes messages received from DRL and messages received from SS7-MPs.

Table 5-6 (Cont.) DM-IWF KPIs

Variable	Description
Diameter-to-MAP Trans Msg Rate	Average number of Diameter-to-MAP transaction messages processed per second.
MAP-to-Diameter Trans Msg Rate	Average number of MAP-to-Diameter transaction messages processed per second.

DP KPIs

Table 5-7 DP KPIs

Variable	Description
DpsQueryRate	Total number of queries received per second
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

GLA KPIs

The KPI values associated with **GLA** are visible using **Main Menu** > **Status & Manage** > **KPIs**

Variable	Description
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on an MP server for this DSR Application. The Ingress Message Rate is the number of ingress Diameter messages that are selected for processing by the ART and sent to the DSR Application for processing.
Success Message Rate	GLA 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 GLA and answered with a success (2xxx) result code).

IDIH KPIs

The KPI values associated with the IDIH will be visible via the GUI **Status & Manage** > **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 **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-8 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

MD-IWF KPIs

The KPI values associated with **MD-IWF** are visible using **Main Menu** > **Status & Manage** > **KPIs**.

Variable	Description
Ingress Message Rate	Average number of MAP-Diameter Interworking messages processed per second on a SS7-MP. Includes MAP msgs received from SS7 network, and Diameter msgs received from DA-MPs.
Diameter-to-MAP Ingress Msg Rate	Average number of MAP-Diameter Interworking messages processed per second that result from Diameter-originated transactions. Includes the initial Diameter Request msg and all resulting MAP msgs that are received.
MAP-to-Diameter Ingress Msg Rate	Average number of MAP-Diameter Interworking messages processed per second that result from MAP-originated transactions. Includes the initial MAP Request msg and all resulting MAP and Diameter msgs that are received.
Diameter Ingress Message Rate	Average number of Diameter messages (both Requests and Answers) received per second from DA-MPs.
MAP Ingress Message Rate	Average number of MAP messages (both requests and responses) received per second from SS7 network.

Message Processor (MP) KPIs

The KPI values associated with **MP** are available using **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-9 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 5-9 (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 **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-10 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 **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-11 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.

Table 5-11 (Cont.) Platform KPIs

Variable	Description
Swap	Percentage utilization of swap space on the server by all software as measured by TPD.
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** > **KPIs**.

Table 5-12 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 5-13 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

Table 5-13 (Cont.) Process-based KPIs

Variable	Description
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
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 5-14 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.

Table 5-14 (Cont.) Provisioning KPIs

Variable	Description
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.
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.

Table 5-14 (Cont.) Provisioning KPIs

Variable	Description
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 **Main Menu** > **Status & Manage** > **KPIs**.

Table 5-15 **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 **Range Based Address Resolution** application.
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.

Subscriber Binding Repository (SBR) KPIs

The KPI values for SBR are visible using **Status & Manage** > **KPIs**.

Table 5-16 SBR KPIs

Variable	Description
SBR Memory Utilization	SBR memory utilization (0-100%)
SBR Process CPU Utilization	SBR Process CPU Percent Utilization (0-100%)

Table 5-17 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
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 5-18 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

SS7/Sigtran KPIs

Table 5-19 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.

Table 5-19 (Cont.) SS7/Sigtran KPIs

Variable	Description
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent.
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received.

DCA Framework KPIs

The KPI values associated with DCA are visible using **Status & Manage** > **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

DCA Custom MEAL KPIs

The KPI values associated with DCA are visible using **Main Menu** > **Status & Manage** > **KPIs**. There are 25 scalar basic templates, 25 scalar Rate templates, 25 arrayed Basic templates, and 25 arrayed Rate templates.

Variable	Description
DcaCustomMeal.name	DcaCustomMeal.kpiDescr

U-SBR KPIs

The KPI values associated with Universal SBR are visible using **Status & Manage** > **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
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